Université de Montréal

La fraude d'identité et la protection des renseignements personnels dans un organisme public

par

David Castonguay

École de criminologie
Faculté des Arts et des Sciences

Rapport de stage présenté à la Faculté des études supérieures
en vue de l'obtention du grade de Maîtrise ès sciences (M.Sc.)
en criminologie

Août 2011

Université de Montréal
Faculté des études supérieures et postdoctorales

Ce rapport de stage :
La fraude d'identité et la protection des renseignements personnels
dans un organisme public

Présenté par :
David Castonguay

a été évalué par un jury composé des personnes suivantes :

Stéphane Leman-Langlois
Président-rapporteur

Benoît Dupont
Directeur de recherche

M.M.J. Lacoursière
Membre du jury

Mémoire accepté le : _____

RÉSUMÉ

Au 21e siècle, les renseignements personnels sont devenus des outils indispensables afin de gérer efficacement les programmes sociaux. Cependant, pour les organisations, la conservation, le traitement et la communication d'une quantité sans cesse grandissante de renseignements personnels représentent des enjeux légaux, notamment en matière de protection à la vie privée, et économiques, complexes. Au cours des dernières années, de nombreux incidents impliquant la perte ou la communication non autorisée de renseignements personnels ont été rendus publics et ils ont mis à jour les difficultés qu'éprouvent les organisations à maintenir la confidentialité des informations qu'elles détiennent.

Dans cette optique, cette recherche permet d'identifier les caractéristiques du phénomène de communication non autorisée de renseignements personnels vécu par un organisme public. Supporté par une base empirique unique comprenant 1 355 cas de tentatives non autorisées d'obtention de renseignements personnels documentés et des rencontres réunissant 19 employés de l'organisation, ce projet présente et analyse les techniques utilisées lors de communication téléphonique par les présumés fraudeurs à la recherche d'informations confidentielles. Concrètement, la communication non autorisée signifie que des personnes prétendant être des clients de l'organisation, des employés, des policiers, des avocats tentent d'obtenir des renseignements précis sur des individus ayant un dossier dans l'organisation.

Loin d'être anodine, la création d'une base de données et l'élaboration de dossiers d'enquête ont permis à la Sûreté du Québec d'arrêter en 2009 une dame qui revendait les renseignements obtenus dans l'organisation à de tierces personnes (avocat, prêteur usuraire, agence de recouvrement). Ces informations préliminaires nous permettent d'avancer qu'il ne s'agit pas d'événements isolés, mais bien de tentatives récurrentes d'obtention illégale de renseignements personnels. Ayant un accès privilégié à ces informations, il nous apparait essentiel d'examiner en profondeur les caractéristiques de ce phénomène pour en comprendre les dynamiques. Par contre, notre projet ne se contente pas d'illustrer la relation binaire entre les présumés fraudeurs et le personnel de l'organisation, mais il cherche à comprendre quels sont les impacts des dynamiques organisationnelles qui caractérisent les centres d'appels sur la structure du phénomène.

À la suite de cette recherche, nous sommes en mesure de dire que les fraudeurs qui parviennent à créer un lien de confiance suffisant, notamment en adoptant une attitude sympathique avec l'agent, ont davantage de succès. Pour y arriver, les présumés fraudeurs utilisent de nombreuses identités; plus de 14 ont été recensés, et plusieurs d'entre elles visent à utiliser une figure d'autorité. Étonnamment, l'utilisation de titres tels qu'avocat ou policier crée l'effet contraire chez les agents. En effet, ces derniers sont plus attentifs et méfiants face à la demande. Enfin, nos résultats semblent indiquer que la pression vécue par les agents liée à la productivité dans les centres d'appel a un impact important sur la protection des renseignements personnels.

Mots clés : protection des renseignements personnels, centre d'appel, ingénierie sociale, accès frauduleux, prévention crime.

ABSTRACT

In the 21st century, personal information has become an essential tool in efficiently managing social programs. However, for the organizations, the conservation, the treatment and the communication of this critical and personal information constantly increases which brings considerable legal stakes, notably in terms of private life protection and economics complex. Over the past years, many incidents involving loss or non-authorized communication of personal information have been publicized. These events illustrate how much difficulty the organizations have in keeping to themselves the confidential information that is given to them.

From this point of view, this research allows to identify the characteristics of the non-authorized communication of personal information phenomenon experienced by a public organism. Indeed, supported by a unique empirical basis containing 1 355 cases of non-authorized attempts to obtain documented personal information and meetings reuniting 19 employees from the organization, this project presents and analyzes the techniques that are used during phone communications by alleged swindlers who were looking for confidential information.

In concrete terms, non-authorized communication means that people pretending to work for the organization, employees, police man, lawyers try to obtain precise information on individuals who have a folder in the organization.

Far from being insignificant, the creation of a data base and the development of an investigative folder allowed the Sûreté du Québec to arrest, in 2009, a woman who was reselling information obtained in the organization to third-parties (lawyer, loaner, and recovery agency). This preliminary information allows us to conclude that these events are not isolated, but recurrent attempts of obtaining illegally personal information. Since we have a privileged access to such information, it appears that it is essential to deeply examine the characteristics of this phenomenon to understand its dynamics. However, our project not only illustrates the binary relation between the alleged swindlers and the organization personnel, but it also tries to understand what the dynamic organizational impacts are on the phenomenon structure.

As a result of this research, we can affirm that the swindlers, who are able to create a sufficient trustworthy connection, notably by adopting a pleasant attitude with the agent, most likely will have success. To achieve that, the alleged swindlers use many identities, over 14 have been counted, and many of them aim to use authority figure. Astonishingly, the use of titles such as lawyers or police man appears to have the opposite effect on the agents while they are the ones who are more attentive and suspicious to the demand. Finally, the results seem to indicate that the pressure lived by the agents related to the productivity of the call centers has an important impact on the protection of personal information.

Key words: protection of personal information, call center, social engineering, fraudulent access, crime prevention.

TABLE DES MATIÈRES

LISTE DES TABLEAUX, GRAPHIQUES ET FIGURES

LISTE DES ABRÉVIATIONS

NAM : Numéro d’assurance maladie

NAS : Numéro d’assurance sociale

LPRP : Loi sur la protection des renseignements personnels

LPRPDE : Loi sur la protection des renseignements personnels et des documents électroniques

CAI : Commission d’accès à l’information

REMERCIEMENTS

Une maîtrise constitue un long parcours qui trouve, selon moi, sa raison d'être à la fois dans le cheminement personnel et professionnel nécessaire pour la terminer que dans la lecture du produit final. Afin d'y arriver, j'ai eu la chance de côtoyer des personnes exceptionnelles qui ont, à leur manière, participées à ce projet. Évidemment, j'aurais pu me simplifier la vie en faisant un projet à la fois, mais ceux qui me connaissent bien savent que je carbure aux défis.

Tout d'abord, merci à mon directeur Monsieur Benoît Dupont, pour ses commentaires qui suscitaient chez moi de nombreuses réflexions et pour sa flexibilité tout au long du projet. Je suis très reconnaissant pour la qualité de tes commentaires et ton attitude positive lors de ces deux années. Ton support, ta compréhension et ta rigueur intellectuelle m'ont grandement motivé. Ensuite, je tiens à remercier spécialement Madame M.M.J. Lacoursière, qui a été ma superviseure de stage lors de ma collecte de données. Sans elle, ce projet n'aurait jamais pu être réalisé. Il ne fait aucun doute que Madame Lacoursière est à l'avant-garde dans sa profession et que sa vaste expérience a été pour moi une source incomparable d'information. J'espère que cette collaboration fût aussi riche pour vous qu'elle le fût pour moi. Je ne pourrais passer sous silence la précieuse collaboration de Madame Durand, directrice adjointe au centre d'appel, qui a grandement facilité mes démarches d'entretien avec les employés.

Un merci spécial à Anouk pour être une conjointe d'exception. Merci de ta compréhension et de ton support incomparable tout au long de ses longues heures de travail en solitaire. Merci de m'avoir écouté lorsque je divaguais sur mes questions de sécurité. À mon rayon de soleil Alyson, tu es la plus belle chose qui m'est arrivée et ta venue m'a apporté une détermination incroyable. Un merci profond à ma famille pour son support inconditionnel et leurs encouragements. Un merci à Marcel pour ton écoute, à Maryse pour m'avoir lu, lu et relu tant de fois au cours de ces années et à Mélissa pour tout ton travail. Merci à mes chums : Xav, Phil, Ben et Max pour m'avoir changé les idées tout au long de ces deux années.

Enfin, merci au CICC pour la bourse de rédaction à laquelle j'ai eu droit afin de m'aider à terminer la rédaction de ce mémoire.

Les personnes qui croient résoudre les problèmes de sécurité par la technologie n'ont ni compris le problème, ni la technologie.
(Schneier, 2000)

INTRODUCTION

La collecte, la conservation et la communication de renseignements personnels[1] ont toujours représenté des enjeux complexes pour la protection de la vie privée. Il ne fait aucun doute que l'utilisation des technologies de l'information a, d'un côté, doté les organisations de la capacité de collecter, de traiter de manière simple et efficace une quantité prodigieuse de renseignements personnels et, de l'autre, considérablement complexifié les défis liés à leur protection. En effet, selon les statistiques officielles collectées par le *Data base loss*[2], un organisme qui recense systématiquement toutes les pertes ou tous les vols de renseignements personnels aux États-Unis, plus de 3 023 cas des pertes de renseignements personnels impliquant 616 448 217 dossiers ont été répertoriés entre 2003 et 2010.

D'après les analyses descriptives effectuées sur ces sources ouvertes, il semblerait que les défaillances dans la protection des renseignements personnels soient généralisées à tous les types d'organisation. En effet, selon Dupont et Gagnon (2009), le secteur public (éducation, services gouvernementaux et la santé) est tout aussi victime de ces incidents que le secteur privé (commerce de détail, industrie, finance). Ces incidents illustrent à la fois le dysfonctionnement des organisations en matière de protection des données personnelles et un intérêt marqué des criminels pour les renseignements personnels. Représentant un potentiel de gain financier non négligeable, les données personnelles sont aujourd'hui une cible attrayante pour les criminels qui n'hésitent pas à user de différents moyens pour les obtenir.

En effet, au cours des dernières années, les médias n'ont pas manqué de souligner les exploits de pirates informatiques talentueux qui parvenaient à obtenir d'un seul coup des millions de renseignements personnels[3]. Les exemples les plus spectaculaires survenus récemment sont ceux d'Albert Gonzalez qui a copié 200 millions de numéros de cartes de

---

1 On entend ici par 'renseignements personnels' ou 'données personnelles' des informations qui permettent d'identifier un individu (nom, âge, adresse civique, numéro de sécurité sociale, numéro d'assurance maladie, etc.), de connaître ses capacités et habitudes de consommation (états des actifs financiers, biens et services achetés, modes de paiement, etc.), son statut à l'égard de certains services publics (dossier fiscal, dossier médical, éligibilité à des programmes sociaux, casier judiciaire, etc.) à l'exception des coordonnées professionnelles de cette personne (titre, adresse commerciale ou numéro de téléphone d'un employé au sein d'une organisation).

2 http://datalossdb.org/

3 Vous pouvez consulter les cas de Cards Systems - Visa, MasterCard, American Express – (2005), TJX Compagnies (2007), RockYou Inc. (2009), Heartland Payment Systems (2009), Sony Corporation (2011).

crédit de client de la compagnie TJX et Sony Corporation qui s'est fait pirater 77 millions de comptes contenant nom, adresse, courriel, date de naissance et modes de paiement de ses utilisateurs.

Cependant, selon Dupont (2010, p. 3), qui a analysé 976 dossiers de pertes ou de vols de données, survenus entre 2005 et 2007, impliquant 313 millions de dossiers personnels, les incidents laissent entrevoir que le piratage est loin de représenter la principale menace. En effet, avec 22,7% des incidents, le piratage ne vient qu'en troisième position derrière la disparition d'équipement (40,1%) et la négligence ou l'erreur humaine (24,7%). Ces résultats laissent croire que le facteur humain dans la protection des renseignements personnels pourrait être plus important que l'on ne pourrait croire. En fait, les organisations font face à une variété de risques menaçant l'intégrité des informations détenues. Il peut s'agir de vol interne, d'erreur, de négligence, de piratage ou de communication non autorisée. Dans ce contexte, ce projet a pour objectif de mettre à jour une menace à la protection des renseignements personnels qui a reçu jusqu'à présent très peu d'attention.

Entre le 1er avril 2006 et le 1er avril 2010, les employés de quatre centres d'appel d'un organisme public ont documenté 1 355 cas de tentatives non autorisées d'obtention de renseignements personnels. Ainsi, des personnes prétendant être des clients de l'organisation, des employés, des policiers, des avocats ont tenté d'obtenir des renseignements précis sur des individus ayant un dossier dans l'organisation. La création d'une base de données et l'élaboration de dossiers d'enquête ont notamment permis à la Sûreté du Québec d'arrêter en 2009 une dame qui revendait les renseignements obtenus dans l'organisation à de tierces personnes (avocat, prêteur usuraire, agence de recouvrement). Pour arriver à ses fins, la dame prétendait être une employée de l'organisme public et utilisait toute sorte de prétextes afin de manipuler les agents[4] des centres d'appel. De plus, selon les informations disponibles, vingt-cinq (25) cas de communication non autorisée de renseignements personnels relatifs à cette fraudeuse ont été portés à l'attention de organisme public lors des deux dernières années. En d'autres termes, lors des deux dernières années, l'organisation a la certitude que lors de ces vingt-

[4] Le terme agent est fréquemment utilisé pour désigner les personnes travaillant dans des centres d'appel.

cinq (25) appels, le fraudeur[5] a réussi à obtenir des renseignements confidentiels sur la clientèle. Ces informations préliminaires nous permettent d'avancer qu'il ne s'agit pas d'événements isolés, mais bien de tentatives récurrentes d'obtention non autorisée de renseignements personnels. Ayant l'autorisation de consulter ces informations pour des fins d'analyse, nous avons jugé essentiel d'examiner en profondeur les caractéristiques de ce phénomène pour en comprendre les dynamiques. Nous avons donc comme objectif principal de dresser un portrait détaillé des stratagèmes utilisés par les présumés fraudeurs lors de communication téléphonique avec l'organisme.

En fait, nous cherchons à comprendre comment ces personnes parviennent à obtenir des renseignements personnels concernant la clientèle de l'organisation. Dans ce projet, nous souhaitons également répondre aux questions suivantes : Quelle est l'ampleur du phénomène pour l'organisation? Comment ce phénomène est-il perçu et géré par le personnel de l'organisation? Est-ce que des éléments présents dans l'organisation facilitent l'obtention non autorisée de renseignements personnels? Quelles sont les pistes de solutions disponibles pour une organisation?

Bien que la communication non autorisée de renseignements personnels, notamment la perte ou le vol de données, reçoive une attention médiatique de plus en plus importante, elle demeure un phénomène peu connu et qui a reçu peu d'attention scientifique, car les organisations sont souvent réticentes à dévoiler ce type d'information. En effet, en plus des conséquences légales, les organisations préfèrent taire ce type d'incident en raison des risques d'atteinte à la réputation et à l'image d'une organisation, des coûts associés à la gestion d'une crise, de la communication individuelle avec les victimes, des enquêtes internes et externes et des amendes et des pénalités. Au Canada, le phénomène est d'autant plus difficile à évaluer car, contrairement aux États-Unis, il ne possède pas de législation obligeant les organisations à déclarer les brèches de sécurité entraînant la perte de renseignements personnels.

---

[5] En fait, il serait plus juste de mentionner «présumé» fraudeur car la personne n'a pas été reconnue coupable de fraude. Cependant, afin de faciliter la lecture et d'alléger le texte, nous allons parler de fraudeur pour désigner le personne qui tente d'obtenir des renseignements personnels.

D’un point de vue social, ces pertes, bien qu’elles n’impliquent pas systématiquement une utilisation criminelle, sont préoccupantes, car le vol d’information n’est habituellement pas une fin en soi, mais plutôt un outil qui facilite ou permet de commettre d’autres crimes tels que la fraude. Ainsi, la perte de renseignements personnels peut être considérée comme la source de multiples problèmes criminels. La population est également de plus en plus inquiète des conséquences directes, notamment financières, et indirectes de la perte de leurs renseignements personnels. Ces incidents amènent aussi l’opinion publique à se questionner quant à l’efficacité des mesures mises en place par les organisations afin de protéger leurs données personnelles. Enfin, la communication non autorisée de renseignements personnels est une menace à la protection de la vie privée, car elle constitue une violation de confidentialité de l’information détenue par les organisations. Conditions préalables au maintien de la liberté et de la démocratie, le droit à la vie privée repose sur une confiance mutuelle entre le citoyen et l’État quant à l’importance et à la valeur de ce droit individuel et commun (*Une question de confiance : Intégrer le droit à la vie privée aux mesures de sécurité publique au 21e siècle*, 2010). Il est donc primordial pour les établissements de mettre en place des mesures qui assurent qu’aucun renseignement personnel n’est communiqué sans autorisation.

Cette recherche permettra de dresser un portrait détaillé d’une menace réelle pour toutes organisations détenant des renseignements personnels, mais dont peu semblent être conscientes. Pour y arriver, nous avons analysé 1 355 rapports d’événement en plus de rencontrer dix-neuf (19) agents d’un centre d’appel. Cette base de données empiriques unique au Québec et possiblement au Canada contient à la fois des informations quantitatives et des informations qualitatives sur la nature du phénomène et la manière dont il est géré par l’organisation. De façon pratique, ce projet identifiera les stratégies utilisées par la majorité des présumés fraudeurs. Ainsi, en améliorant les connaissances sur le phénomène, nous souhaitons apporter une contribution embryonnaire dans la mise en place des stratégies de protection efficaces des renseignements personnels au Québec.

Ce mémoire est divisé en quatre chapitres. Dans un premier temps, nous dresserons un bilan des connaissances sur la protection des renseignements personnels. En raison du manque de recherches empiriques sur cette problématique spécifique, nous avons dû

réunir quatre littératures différentes afin d'offrir un aperçu juste du phénomène et de ses enjeux.

Dans un second temps, nous décrirons la méthodologie employée afin de répondre à nos objectifs de recherche. Il importe de préciser que bien que nous ayons utilisé des informations de nature quantitative, la grande majorité des analyses est basée sur des données qualitatives recueillies soit lors des entretiens ou dans les fiches de signalement complétées par les agents. Ce projet de recherche a eu lieu dans une grande organisation publique qui possède plusieurs unités administratives et différents centres d'appel au Québec.

Le troisième chapitre sera consacré à la présentation des résultats. Celui-ci sera divisé en quatre grandes sections. La première décrira les principales mesures administratives mises en place par l'organisation afin de protéger les renseignements personnels. La seconde partie exposera l'ampleur du phénomène pour l'organisation. La troisième section présentera une séquence d'interaction entre le présumé fraudeur et l'agent que nous avons développée afin de présenter les éléments présents dans la grande majorité des tentatives non autorisées d'obtention de renseignements personnels. Pour créer cette séquence, nous nous sommes inspirés du concept de script développé par Cornish (1994). Quant à la dernière partie, elle portera sur les éléments individuels et organisationnels influençant l'opportunité d'obtention de renseignements personnels.

Dans le quatrième chapitre, nous utilisons les résultats présentés dans la section précédente afin de les mettre en perspective dans un cadre plus large et d'en tirer des leçons. Nous présenterons également des pistes de solutions afin d'améliorer la protection des renseignements personnels.

CHAPITRE I :

LA COMPLEXITÉ DE LA PROTECTION

DES RENSEIGNEMENTS PERSONNELS

Le phénomène du vol de renseignements personnels a reçu jusqu'à présent peu d'attention scientifique. Cette absence de connaissance est, entre autres, due au fait que les organisations sont réticentes à partager les informations sur les situations où des renseignements personnels ont été perdus ou parce que les pertes sont survenues à leur insu. Ainsi, il nous est impossible de mettre en perspective les résultats de différentes études sur le sujet. Afin d'obtenir un portrait clair du phénomène, nous avons donc réuni quatre littératures qui n'ont pas l'habitude de coexister. En effet, cette recherche est unique dans la mesure où elle intègre à la fois des notions théoriques de la criminologie, de la sociologie des organisations, de la psychologie cognitive et de l'informatique.

D'entrée de jeu, nous utiliserons les bases théoriques de la notion d'opportunité criminelle, développée en criminologie, comme fondation de notre revue de la littérature. Le concept d'opportunité nous permettra de mettre en relation trois éléments qui nous semblent essentiels à la mise en contexte du phénomène soit, une cible intéressante à voler, un gardien responsable de sa protection et un délinquant motivé. Par la suite, la sociologie des organisations nous permettra de saisir le contexte organisationnel dans lequel le phénomène a lieu. Quant à la psychologie cognitive, elle nous renseignera sur les ambigüités du traitement de l'information chez l'humain et sur les erreurs de jugement exploitées par les présumés fraudeurs. Finalement, nous utiliserons les écrits en informatique, car ils contiennent une littérature émergente et fascinante sur le rôle capital que joue l'humain en matière de protection de l'information.

Notre recension des écrits se présente comme suit. Dans un premier temps, nous traçons les principales caractéristiques de la société de l'information ainsi que les enjeux qui en émergent en matière de protection des renseignements personnels. Dans un second temps, nous définirons les composantes de la théorie des opportunités criminelles. Nous amorcerons par la présentation des caractéristiques de la cible. Par la suite, nous exposerons le contexte organisationnel dans lequel évolue l'agent responsable de protéger la cible. Enfin, nous présenterons les différentes stratégies qu'utilise le délinquant.

1. LA RÉVOLUTION INFORMATIONNELLE

Les enjeux liés à la protection des renseignements personnels s'inscrivent dans un contexte social qui a connu de nombreux changements lors des dernières années. Parmi ceux-ci, l'avènement du traitement numérique des données et du développement des réseaux informatiques a profondément bouleversé la structure des échanges sociaux et économiques. En effet, au 21e siècle, les technologies de l'information et de la communication[6] (TIC) sont des composantes essentielles des économies contemporaines et une source majeure de dynamisme pour les sociétés, car elles ont, entre autres, permis de faire disparaître les frontières de l'espace et du temps qui définissaient autrefois les interactions sociales. L'utilisation progressive des technologies de l'information par l'ensemble des secteurs économiques, a redéfini les modes de communication, de production et de consommation, mais également la manière d'offrir des services (Curien & Muet, 2004, p. 9).

Effectivement, on remarque depuis une quarantaine d'années que les institutions publiques ainsi que les entreprises privées ont considérablement augmenté le nombre de services offerts à leur clientèle par l'entremise des TICs. La tendance du gouvernement en ligne (*e-gouvernement),* auquelle nous assistons présentement, est le fruit d'une longue évolution qui a commencé, notamment par le téléphone, et qui s'est accéléré avec le développement de l'informatique et d'Internet. Pour les institutions publiques, cette évolution, à la fois guidée par le développement des TICs, la familiarisation des usagers aux systèmes et par une volonté de rationaliser les opérations, le personnel et les finances publiques, s'est traduite par un changement radical dans la manière dont les services sont offerts à la population.

Comme le souligne le sociologue américain Manuel Castells[7], les nouvelles technologies, qui proviennent principalement de Silicon Valley pendant les années 1970, sont la source même de changements sociaux, perçus comme historiques et planétaires, ainsi que des transformations de la structure de l'économie, de la stratification sociale, de la politique et de la culture. Si les innovations technologiques telles que la radio, la télévision, le téléphone, les vidéos, le cellulaire,

---

6 Nous entendons par TIC, les appareils et les techniques qui permettent de traiter et de transmettre des informations. Par exemple : l'informatique, l'Internet et les télécommunications.

7 Les travaux du sociologue américain Manuel Castells, *L'ère de l'information* (Tome 1 : La société en réseau, Tome 2 : Le pouvoir de l'identité et Tome 3 : Fin de millénaire), sont sans contredit ceux qui proposent l'argumentation la plus élaborée sur l'impact du développement des technologies de l'information et de la communication dans les sociétés postmodernes.

l'ordinateur ou le GPS, sont le moteur d'une hyperconsommation, il est indéniable qu'elles ont transformé le fonctionnement des organisations. Ces innovations ont, entre autres, doté les organisations d'une capacité technologique et organisationnelle de traiter et d'échanger une quantité d'information presque illimitée. Libres des contraintes physiques qui régissaient autrefois leurs opérations, les organisations ont commencé à collecter une quantité impressionnante d'information. Rapidement, les renseignements personnels ont été ciblés par les organisations en raison du potentiel économique qu'ils représentent.

Dans ce nouveau contexte où l'information occupe une place prépondérante, les organisations se démarquent par leur capacité à utiliser les renseignements personnels afin d'améliorer leurs produits et leurs services. À titre d'exemple, pour le gouvernement, la création de bases de données nationales permet d'administrer plus efficacement et justement les programmes sociaux. Ces bases de données nationales peuvent également contribuer à la sécurité nationale en permettant une identification plus rapide et détaillée des citoyens. Des pays tels que l'Espagne, l'Autriche et la Belgique utilisent déjà des cartes d'identité nationales électroniques. Dans le même ordre d'idées, de plus en plus de pays discutent de la possibilité de créer des cartes d'identité contenant des éléments biométriques afin d'effectuer un contrôle plus efficace sur les personnes.

Au sein de l'industrie privée, l'utilisation des informations sur les transactions de la clientèle procure aux organisations, des données brutes extrêmement puissantes qui permettent d'analyser les tendances et les comportements ainsi que de dresser des profils de consommateurs et d'améliorer la qualité et l'efficacité du service offert mais également d'influencer le comportement du consommateur. Dans le secteur financier, il est possible d'appliquer une autre logique à l'utilisation de renseignements personnels. En effet, les renseignements personnels sont un outil essentiel dans la lutte contre le blanchiment d'argent et la fraude. Ainsi, on remarque que peu importe la sphère économique ou sociale dans laquelle une organisation évolue, la collecte et la conservation d'un maximum d'information ont eu pour conséquence directe une multiplication des bases de données.

1.1. La divulgation d'information personnelle, une condition d'accès aux services

Dans un contexte social où de plus en plus de transactions se font par téléphone ou en ligne, les citoyens sont appelés, presque quotidiennement, à communiquer des renseignements personnels afin de prouver leur identité. On peut distinguer trois catégories de données personnelles. Tout d'abord, il y a les informations qui permettent d'identifier un individu (nom, âge, adresse, nom des parents, lieu de naissance, ADN, rétine, empreinte, signature). Ensuite, il y a les informations distribuées par les organisations (numéro d'assurance sociale, numéro d'assurance maladie, code permanent, numéro d'employé, numéro de client). Ces informations devraient seulement être utilisées dans la relation avec l'organisation émettrice. Enfin, la troisième catégorie regroupe les données sur le statut et les moyens de la personne (dossier fiscal, dossier médical, casier judiciaire, éligibilité à des programmes sociaux, état des actifs financiers, mode de paiement). Les clients contactent souvent les centres d'appel afin d'obtenir ces informations. Aujourd'hui, si une personne désire communiquer avec un organisme public, elle devra absolument divulguer des renseignements personnels afin d'avoir accès à des services et à des informations concernant son dossier.

Les protocoles d'identification constituent une norme en matière de sécurité essentielle permettant d'assurer une confidentialité de l'information et la protection de la vie privée[8]. Bien qu'il diffère d'une organisation à l'autre, un protocole comprend généralement une série de questions qui exigent du client de communiquer des renseignements personnels le concernant. L'accumulation des preuves d'identité permettra à l'organisation de certifier qu'il s'agit de la bonne personne (Jones & Levi, 2000). Cependant, il importe de souligner que lors de communication téléphonique, l'authentification de l'identité comporte de nombreux défis, car il est impossible de valider l'authenticité visuelle des documents que possède le requérant. Le processus d'authentification est, par conséquent, beaucoup plus complexe et vulnérable que s'il était réalisé en personne.

Quotidiennement, si l'identification consiste à connaître le nom de la personne et ses caractéristiques physiques, on constate qu'à l'ère de l'information, les procédures afin d'identifier

[8] La protection de la vie privée a toujours été un droit fondamental dans les sociétés occidentales. Au Canada, elle est présente dans la Déclaration universelle des droits de l'homme de 1948 et dans la Charte canadienne des droits et libertés.

les personnes, ainsi que les circonstances dans lesquelles s'effectue l'authentification de l'identité, ont changé. En effet, dans ce contexte mondial où les échanges sociaux et économiques sont devenus impersonnels, l'identification est de plus en plus fréquente et elle repose moins sur des liens personnels, et davantage sur des éléments d'information que, en théorie, seule la personne devrait connaître ou posséder (*Lignes directrices en matière d'identification et d'authentification*, 2006).

Il ne fait aucun doute que les protocoles d'identification contribuent à la protection de la vie privée, car ils réduisent les risques de communication de renseignements personnels à des personnes qui ne sont pas autorisées à obtenir cette information. Cependant, ils doivent être conçus en tenant compte de la nature de l'information demandée et des risques qui sont associés à cette information. Les organisations ne peuvent pas toutes exiger que leur clientèle s'identifie en communiquant l'ensemble de leurs renseignements personnels, car au sein du concept de vie privée se trouve celui de l'anonymat. Cet élément clé signifie, entre autres, qu'il est convenu que seules des raisons valables doivent obliger une personne à s'identifier. Bien que certaines organisations gouvernementales ou des entreprises privées, telles que les institutions financières, se doivent de refuser l'anonymat (*Lignes directrices en matière d'identification et d'authentification*, 2006), on remarque que plusieurs organisations exigent illégitimement, souvent pour des raisons de sécurité, des renseignements personnels afin de confirmer l'identité du requérant. Bref, l'application de systèmes d'identification exige l'atteinte d'un équilibre dont la nature est délicate, car un protocole trop rigoureux peut conduire à une invasion de la vie privée et un protocole trop simple ne protège pas efficacement l'information du client.

Rapidement, on réalise que l'identification est devenue la base des échanges entre les citoyens et les organisations privées et publiques. Par conséquent, l'utilisation de renseignements personnels est indispensable au bon fonctionnement de ces échanges. Considérée comme une condition d'accès aux services, l'identification des personnes est un besoin social et économique qui stimule inévitablement la collecte, l'utilisation et la communication d'identifiants personnels (Marx, 2001, p. 311). Paradoxalement, on remarque que les besoins de protection des renseignements personnels ont un effet pervers de stimuler la collecte de renseignements. Ainsi, les besoins de sécurité stimuleraient une collecte indue de renseignements personnels au détriment de la vie privée.

1.2. La vie privée et la protection des renseignements personnels

Nous avons vu que la collecte et l'utilisation de renseignements personnels à des fins d'identification permettent d'assurer la confidentialité de l'information. Cependant, cette tendance lourde amène également de nouveaux risques. Halperin et Backhouse (2008, p.73) soulignent qu'il émerge de cette tendance une tension entre les concepts de sécurité et de protection de la vie privée[9]. Ainsi, nous soulèverons trois enjeux qui caractérisent la société de l'information, soit la capacité et la volonté de protéger les renseignements personnels ainsi que l'utilisation qui en est faite.

Le premier enjeu concerne la gestion des accès aux renseignements personnels. En effet, la collecte et le stockage d'informations personnelles amènent des questionnements quant à la capacité des organisations d'en assurer la protection et la confidentialité. Bien que les bénéfices d'une telle pratique pour les citoyens, les entreprises et les gouvernements soient relativement simples à saisir, de nombreux incidents impliquant la perte ou le vol d'informations personnelles démontrent les risques qu'elle représente. Aux États-Unis, 3 623 cas impliquant 616 448 217 dossiers ont été rendus publics entre 2004 et 2010. Utilisant sensiblement les mêmes sources, Dupont et Gagnon (2009, p. 5) notent, dans leur analyse de 976 incidents impliquant la perte ou le vol de données personnelles entre 2005 et 2008, un déficit manifeste et systématique de sécurité en ce qui concerne la collecte, le traitement, le stockage et la gestion de l'informatique. En plus, au cours des dernières années, l'augmentation considérable de la puissance et la miniaturisation des moyens de stockage signifient que les mouvements ou les flux de données personnelles sont beaucoup plus difficiles à sécuriser. En fait, l'information numérique par sa forme intangible et sa quantité constitue un bien très difficile à protéger. Bref, les informations disponibles permettent de mettre en doute la capacité des organisations à protéger efficacement les renseignements personnels qu'elles collectent.

Le domaine de la santé est un bon exemple des risques et des défis de la gestion des accès aux renseignements personnels. Il est indéniable que la numérisation de l'information et le partage de celle-ci à travers tous les services de santé provinciaux et municipaux, privés ou publics, permettraient d'offrir un service de meilleure qualité aux citoyens. Cependant, lorsque l'on

[9] Au Canada, la protection de la vie privée est une valeur sociale, collective et juridique importante. Il s'agit, entre autres d'un droit garanti par la Charte canadienne des droits et libertés.

s'attarde à la question de l'accès à ces bases de données, on réalise qu'il est quasi impossible de garantir que les renseignements personnels resteront confidentiels. Bref, les organisations font face à un dilemme entre les bénéfices d'une telle pratique et les risques qu'elle représente. Ce constat permet de mettre en perspective les risques de cette tendance qui caractérise la société de l'information.

Le second enjeu concerne la volonté des organisations à protéger les renseignements personnels de leurs clients. En l'absence de contraintes technologiques, plusieurs organisations collectent beaucoup plus qu'elles en ont réellement besoin. Dans une minorité de cas, ces données sont réellement utilisées par l'organisation. Collectées inutilement, ces informations sont dormantes et elles représentent peu d'intérêt pour l'organisation. Ainsi, peu d'effort et de mesures sont mis en place par les organisations pour les protéger.

Le troisième enjeu provient de la manière dont les renseignements personnels sont utilisés. Car une fois qu'une organisation a collecté l'information, elle peut pratiquement en faire ce qu'elle veut. Par exemple, dans la lutte contre le crime, et plus particulièrement dans celle contre le terrorisme, l'utilisation de renseignements personnels sans le consentement de la personne peut illustrer l'érosion de la vie privée au détriment des besoins de sécurité. Ainsi, les besoins de sécurité primeraient sur le droit à la vie privée. Des recherches ont argumenté que cette collecte systématique de renseignements personnels symbolisait une tendance vers une société de surveillance[10] (Marx, 1988; Taylor, Lips, & Organ, 2008). Déjà en 1988, Marx (1988, p. 178) remarquait que l'enregistrement systématique de toutes les transactions entre le citoyen et le gouvernement ou les entreprises privées contribuaient à une surveillance routinière, élargie et approfondie.

Cependant, la sécurité et la vie privée ne sont pas toujours en opposition (Halperin & Backhouse, 2008, p. 73). Lors des dernières années, dans plusieurs pays occidentaux qui encouragent l'intervention de l'État, plusieurs limites légales ont été imposées à la surveillance au nom du droit à la vie privée. De l'autre côté, il est indéniable que la protection de l'information ne peut pas être assurée sans un certain niveau de mesures technologiques et organisationnelles. En d'autres termes, la protection de la vie privée ne peut pas être assurée sans des mesures de

[10] Voir aussi Oscar H. Gandy Jr. (1989)et David Lyon (1994).

sécurité. Donc, il serait faux de croire que la sécurité et la vie privée représentent une dichotomie claire, car elles contribuent, dans une certaine mesure, toutes les deux l'une à l'autre (Halperin & Backhouse, 2008, p. 73).

1.3. Le cadre légal

Afin de limiter la collecte systématique de renseignements personnels, le gouvernement fédéral[11] a mis en place en 1985, la *Loi sur la protection des renseignements personnels* (LPRP). À l'époque, cette loi encadrait spécifiquement la collecte, l'utilisation et la communication de renseignements personnels par les institutions fédérales. Cependant, l'augmentation rapide de la quantité et de la précision des informations personnelles collectées par les autres organisations publiques, mais également par les organisations privées, a obligé le gouvernement à apporter des modifications législatives. Ainsi, en 2001, tous les secteurs des activités commerciales, des services et de la fabrication ont été encadrés dans ce que l'on nomme la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDÉ). Celle-ci impose des obligations en matière de gestion et de protection des renseignements personnels à plus de 250 ministères et organismes fédéraux en limitant la collecte, l'utilisation et la communication de renseignements personnels.

Au Canada, le principal acteur est le commissariat à la protection de la vie privée. Créer en 1977, le Commissariat agit en tant que mandataire indépendant du Parlement et son rôle est de valoriser la protection de la vie privée en publiant des rapports, en surveillant les tendances en matière de protection de la vie privée, en soutenant la sensibilisation du public et en fournissant des opinions juridiques. Cependant, cet organisme n'a pas seulement un rôle de spectateur. En effet, le commissariat a également une capacité coercitive dans la mesure où il examine les plaintes des citoyens, évalue la conformité des organisations et intente des poursuites (www.priv.gc.ca).

Au Québec, l'Assemblée nationale a créé en 1982 la Commission d'accès à l'information (CAI). Véritable pionnière en Amérique du Nord en matière d'accès à l'information et de protection de la vie privée, la commission est en charge d'administrer la *Loi sur l'accès aux documents des*

[11] La responsabilité en matière de protection des renseignements personnels est mixe entre le fédéral et le provincial. Plusieurs provinces, dont la Colombie-Britannique, l'Alberta et le Québec, se sont dotées d'un cadre légal spécifique et d'institution en charge de leur application. Par contre, toutes ces lois s'harmonisent avec le cadre légal élaboré par le gouvernement fédéral.

organismes publics et sur la protection des renseignements personnel (L.R.Q., c. A-2.1). Par la suite, le 1er janvier 1994, le législateur québécois innove en imposant également une obligation de protection des renseignements personnels au secteur privé[12] et l'application de la loi est assignée à la CAI. Aujourd'hui, la commission a pour mandat de promouvoir l'accès aux documents des organismes publics et la protection des renseignements personnels dans les secteurs publics et privés, d'en assurer la surveillance et de décider des demandes de révision qui lui sont présentées (www.cai.gouv.qc.ca).

Certes, la société de l'information n'a pas créé la plupart des enjeux qui existent aujourd'hui, mais elle a augmenté significativement leurs importances (Newman, 2008, p. 10). L'usurpation d'identité[13] est un bon exemple. Ce crime qui consiste à se faire passer pour une autre personne, vivante ou morte, afin d'obtenir un avantage, d'obtenir un bien, de causer un désavantage à une personne ou d'éviter une arrestation ou une poursuite, est très ancien. Cependant, au 21e siècle, cette forme de criminalité tire profit non seulement des innovations technologiques qui permettent aux délinquants d'utiliser des machines qui ont la capacité de livrer des quantités importantes d'éléments identificateurs en temps réel, mais également de la prolifération du nombre de renseignements personnels et du rôle accru qu'ils occupent dans la société. Dorénavant essentiels au bon fonctionnement social et économique, les renseignements personnels deviennent des clés dans les interactions avec les entités privées, notamment les institutions financières et le gouvernement.

Ainsi, en plaçant les informations personnelles à l'avant-plan des interactions sociales et économiques des sociétés modernes, les éléments identificateurs composant l'identité sont devenus des cibles intéressantes pour les voleurs au même titre qu'une voiture ou une télévision (Newman, 2008). Si, à la suite de la Seconde Guerre mondiale, la libre circulation des biens et des personnes ainsi que la désertion des domiciles, ont engendré une augmentation des délits d'appropriation (Cohen & Felson, 1979), il est possible que le nouveau rôle accru des renseignements personnels dans nos sociétés ait créé de nouvelles opportunités criminelles. Dans les prochaines pages, il sera pertinent d'identifier les éléments qui structurent l'opportunité de vol de renseignements personnels.

---

[12] *Loi sur la protection des renseignements personnels dans le secteur privé* (L.R.Q., c. P-39.1).

[13] Les termes impersonnification ou fraude d'identité sont également utilisés.

2. UNE CONCEPTION STRATÉGIQUE DE L'OPPORTUNITÉ DU VOL DE RENSEIGNEMENTS PERSONNELS

2.1. L'analyse stratégique

Depuis les années 1980, une attention particulière a été accordée en criminologie au passage à l'acte (Clarke, 1995, p. 2; Clarke & Cornish, 1985, p. 152; Cornish, 1994). Ainsi, à l'époque, Mayhew, Clarke, Sturman et Hough (1975) ont avancé que le crime était avant tout le résultat d'une opportunité influencée par des variables situationnelles. Par la suite, les travaux des Américains Cohen et Felson (1979) ont montré statistiquement que les variations de la criminalité correspondaient à l'évolution de la quantité d'opportunités criminelles s'offrant aux délinquants potentiels. Ils ont alors défini l'opportunité criminelle comme la convergence dans le temps et dans l'espace d'une cible intéressante, d'un délinquant motivé et de l'absence d'un gardien capable de protéger la cible (Cohen & Felson, 1979, p. 604). Il s'agit d'un changement de paradigme important qui aura un impact considérable sur la manière de concevoir les problèmes criminels, car l'intérêt n'est plus tant les caractéristiques personnelles du délinquant que les particularités du délit qu'il commet. On cherche alors à identifier les conditions rendant un crime possible et attirant pour le délinquant. En identifiant ces composantes, les chercheurs souhaitent pouvoir mettre en place des mesures pour réduire le crime[14].

Au Québec, ce courant de recherche est mieux connu sous le nom d'analyse stratégique[15] (Cusson & Cordeau, 1994, p. 7). Cette approche s'intéresse à la fois aux circonstances qui favorisent ou empêchent la perpétration d'un délit et aux stratagèmes mis en œuvre par le délinquant afin d'arriver à ses fins. L'analyse stratégique comporte une série de postulats, dont celui de la rationalité limitée, de la réciprocité et des tactiques criminelles, que nous appliquerons à la littérature sur le vol de renseignements personnels.

2.1.1. La rationalité

Le concept de la rationalité signifie que les actions du criminel ne sont pas le résultat de prédisposition physiologique au crime, mais bien le fruit d'une démarche rationnelle lui

---

[14] Ce changement de paradigme est accompagné d'une transformation générale dans la manière dont la société conçoit le crime et le criminel. On assiste à une prise de conscience du risque inhérent aux sociétés modernes face au crime qui implique que la société accepte ce risque et qu'elle doit mettre en place différentes mesures pour le gérer. Ceci fait référence au concept de société du risque inventé par Ulrich Beck (1992).

[15] Les pays anglo-saxons la définissent comme *rational choice approach* (Cornish, Clarke, 1986).

permettant de maximiser ses gains tout en minimisant ses coûts (Clarke & Cornish, 1985). Ainsi, le crime est un comportement orienté vers des résultats, ayant sa rationalité propre, compte tenu des opportunités qui s'offrent à l'acteur et de la conduite de ses adversaires (Cusson, 1989, pp. 76-77). Dans notre recherche, l'objectif du présumé fraudeur qui usurpe l'identité d'une personne est d'obtenir des renseignements personnels sans droit. Cependant, notre compréhension de cette finalité ne peut pas dépasser cette interprétation en raison des informations limitées que nous possédons sur les personnes commettant ce délit. Nous serons tout de même en mesure de soulever des pistes d'interprétation quant aux motivations de cette forme de criminalité grâce à la littérature sur le sujet.

Nous considérons qu'il est d'autant plus pertinent d'utiliser le postulat de la rationalité criminelle qu'il semble difficile de nier que la commission de ce type de fraude nécessite un minimum de préparation. En effet, le fraudeur doit réunir les informations qu'il possède sur sa victime, il va probablement se pratiquer et répéter des scénarios. Dans cette optique, la démarche du criminel est rationnelle et vise à maximiser ses chances de succès.

Cependant, nous sommes conscients que cette rationalité n'est pas totale et qu'elle peut être altérée ou limitée par les caractéristiques individuelles du criminel ou selon les informations dont il dispose (Cornish & Clarke, 1986; Cusson, 1986). Le délinquant peut baser ses actions sur de fausses représentations de la réalité, des spéculations tout en négligeant d'autres informations pertinentes. Pour employer les termes de Simon (1982), il serait donc plus juste de parler de rationalité subjective dans la mesure où les actions du délinquant peuvent être le résultat d'un traitement rationnel, mais imparfait de l'information. Dans le même ordre d'idées, il est primordial, selon nous, d'appliquer le postulat de la rationalité limitée au gardien. En effet, il est très rare que le gardien possède, lui aussi, toutes les informations possibles et qu'il prenne dans toutes les situations, la décision optimale. Ainsi, la littérature sur la sociologie des centres d'appel et la psychologie cognitive, nous permettrons d'identifier une série de contraintes organisationnelles et individuelles qui influencent la prise de décision des agents.

2.1.2. La réciprocité

Il ne fait aucun doute que le phénomène criminel est un acte conflictuel entre un criminel et un gardien ou une cible. L'analyse stratégique s'intéresse particulièrement à cette interaction entre les protagonistes, délinquant et victime ou délinquant et forces de l'ordre, afin de comprendre comment ils adaptent mutuellement leurs actions aux réponses de l'autre.

Pour notre étude, toutes les tentatives de vol de renseignements personnels sont le résultat d'une interaction entre le fraudeur et l'agent. Lors de communication téléphonique, le fraudeur est en communication directe avec le gardien. Ce dernier posera une série de questions afin de confirmer l'identité de la personne. Le fraudeur doit prévoir les questions de l'agent et préparer des réponses crédibles. Si le fraudeur n'est pas en mesure de répondre correctement aux questions ou s'il n'a pas de justification plausible, l'agent lui refusera l'accès au dossier. De leur côté, en plus de recevoir une courte formation sur la gestion des appels suspects, les agents partagent les cas de fraude vécus ainsi que les stratagèmes utilisés par les fraudeurs. Ainsi, le prochain agent qui fera face à ce stratagème pourra réagir efficacement. Bref, les actions du fraudeur et le déroulement de la fraude sont sans doute tributaires des réactions et des interventions de l'agent (voir Blum, 1972). Nous analyserons cette interaction dans le chapitre 4.

2.1.3. Les tactiques criminelles

Dans la mesure où l'interaction entre le présumé fraudeur et l'agent est au centre des tentatives d'obtention de renseignements personnels, il est pertinent d'identifier les tactiques utilisées par le fraudeur pour déjouer l'agent. Dans le cadre de l'analyse stratégique, Cusson et Cordeau (1994, p. 96) utilisent la notion de tactiques criminelles : « c'est la séquence des choix et gestes posés par le délinquant durant les faits : la manière dont il combine les moyens disponibles pour réaliser ses fins tout en s'adaptant aux circonstances ». En identifiant les stratégies employées par la majorité des fraudeurs, nous souhaitons comprendre le moment du crime et le processus dans lequel il s'inscrit. Cela nous permettra aussi de rendre compte du déroulement de l'interaction entre le criminel et le gardien, mais également d'identifier des éléments de l'environnement présents au moment du crime qui favorisent ou réduisent sa commission.

En raison des informations limitées que nous possédons sur les étapes préalables au crime, notre attention est portée sur les étapes d'exécution et non sur celle de la préparation. Par le fait même, nous considérons que les variables situationnelles influencent avant tout le succès ou l'échec du

vol de renseignement et non pas le processus décisionnel du criminel à passer à l'acte ou non. Selon nous, lorsque le fraudeur communique avec l'organisme public, il a déjà pris la décision de passer à l'acte. Par contre, comme nous l'avons mentionné, le déroulement de l'interaction avec l'agent des centres d'appel influencera les tactiques que le fraudeur utilisera et cela n'empêche pas que les variables situationnelles jouent un rôle déterminant dans le déroulement de l'action. Cette interprétation du rôle des variables situationnelles diffère quelque peu de ce que nous retrouvons dans la littérature.

2.1.4. L'étape de l'acquisition de l'information

La littérature scientifique identifie trois étapes distinctes[16], mais complémentaires aux crimes reliés au vol de renseignements personnels (Sproule & Archer, 2008). Il y a d'abord l'acquisition, qui consiste à voler les informations personnelles appartenant à une personne vivante ou morte. Par la suite, les informations volées vont être soit revendues sur des marchés illicites où la loi de l'offre et de la demande va permettre d'en déterminer la valeur d'usage, soit elles vont être utilisées afin de créer des identités synthétiques (Dupont & Louis, 2009, p. 6). Enfin, la dernière étape consiste à utiliser les informations volées pour effectuer la fraude proprement dite. Il peut s'agir d'encaisser un chèque frauduleux, d'ouvrir un compte bancaire, d'avoir un prêt personnel, d'avoir accès illégalement à des biens ou services, de faire de l'immigration illégale ou de terrorisme (Sproule & Archer, 2006).

Cette recherche s'intéresse particulièrement à l'étape d'acquisition. Afin de bien distinguer les composantes de cette étape, nous identifierons qui peut voler des renseignements personnels, que vole-t-il et comment les vole-t-il. Tout d'abord, le voleur peut être un étranger, un membre de la famille, un collègue de travail, un ami, une connaissance ou un employé ayant un accès privilégié à des renseignements personnels. Ensuite, la cible du voleur peut être des documents physiques (carte de crédit, carte de débit, permis de conduire, carte d'assurance maladie, extrait de naissance, courrier, chèque personnel, carte d'assurance sociale, etc.) ou des informations (numéro d'assurance sociale, information sur la carte de crédit, information sur le compte bancaire, niveau endettement, situation familiale, nom et adresse, date de naissance, condition médicale, statut au sein d'une organisation, mot de passe, etc.). Enfin, les méthodes d'acquisition peuvent être techniques (pirater une base de données ou un mot de passe), physiques (vol, perte,

[16] Cette distinction en trois étapes distinctes est également présente dans le code criminel.

fouille de poubelle, infiltration d'employé) ou par l'ingénierie sociale (*phishing*, fraude 419, demande frauduleuse par téléphone ou en personne, manipulation d'un employé) (Dupont & Louis, 2009, p. 7; Sproule & Archer, 2006).

Selon les études empiriques sur le vol d'identité, les modes d'acquisition privilégiés sont le vol physique et l'utilisation frauduleuse d'un fichier (Dupont & Louis, 2009, p. 12). Selon Gordon, Rebovich, Choo & Gordon (2007), qui ont analysé avec le soutien du service secret américain, l'une des principales organisations d'application de la loi fédérale engagée dans la lutte contre le vol d'identité aux États-Unis, 517 cas de vol d'identité impliquant 933 personnes, 41% des criminels n'ont utilisé aucun dispositif technologique pour commettre leur délit. De plus, Copes et Vieraitis (2007, p. 38), soulignent que l'achat d'information volée est également un mode d'acquisition utilisé, car il est relativement simple et sans risque. Enfin, dans une étude analysant vingt-trois (23) groupes de fraudeurs de chèques œuvrant dans la région de Montréal entre 1991 et 1996, Lacoste et Tremblay (2003, pp. 180-181) notent que neuf (9) groupes se procuraient l'information en volant du courrier. Bref, plusieurs études arrivent à la conclusion que la majorité des vols de renseignements personnels ne sont pas technologiques, voire même, plutôt rudimentaires (Berg, 2008, p. 153; Copes & Vieraitis, 2007; Dupont & Louis, 2009). Cette conclusion modifie la manière de concevoir la menace ainsi que les moyens de protection à mettre en place pour s'en protéger.

3. L'OPPORTUNITÉ DE VOL DE RENSEIGNEMENTS PERSONNELS

Comme nous l'avons mentionné, les écrits criminologiques ont avancé que le crime était avant tout le résultat d'une opportunité influencée par des variables situationnelles. Cohen et Felson (1979) définissent l'opportunité criminelle comme la convergence dans le temps et dans l'espace d'une cible intéressante, d'un délinquant motivé et de l'absence d'un gardien capable de protéger la cible. Ainsi, nous utiliserons ces éléments théoriques incontournables afin de structurer notre présentation des connaissances sur le vol de renseignements personnels.

Pour cette étude, la cible est les renseignements personnels des clients de l'organisation et le fraudeur est le délinquant qui constitue la menace. Au milieu de ceux-ci, se trouve le gardien, c'est-à-dire l'agent des centres d'appel qui a, entre autres, pour responsabilité de protéger les

renseignements personnels et d'offrir un service à la clientèle. Cependant, comme le souligne Ronald V. Clarke (1995, p. 14), la structure des opportunités criminelles est un enjeu d'interdépendance et d'influence complexe entre les criminels, les cibles potentielles et les gardiens. Ainsi, une présentation statique des trois éléments de base composant l'opportunité criminelle n'illustrerait pas fidèlement la complexité du phénomène de vol de renseignements personnels.

Considérant que le crime entretient une relation étroite avec son environnement (Brantingham & Brantingham, 1993) et que les centres d'appel constituent notre environnement de recherche, nous intégrerons la littérature sur la sociologie des organisations afin d'identifier les éléments de l'environnement qui favorisent ou réduisent le vol de renseignements personnels lors de communication téléphonique. Par la suite, les écrits sur la psychologie cognitive nous permettront de comprendre comment le fraudeur exploite l'interaction avec l'agent des centres d'appel.

3.1. Les renseignements personnels, une cible intéressante

3.1.1. Les éléments identificateurs

Lors de vol de renseignements personnels, les cibles sont des pièces d'identité d'une personne. D'entrée de jeu, il est nécessaire de faire une distinction importante entre l'identité comme tout et les éléments identificateurs comme manifestation concrète de cette identité. En effet, lorsqu'une personne vole des renseignements personnels, elle ne vole pas l'identité de la personne, mais bien des pièces de celle-ci. L'identité est une notion complexe et multidisciplinaire qui est en constante évolution (Rannenberg, 2009, p. 19)[17]. Afin d'aborder cette notion d'identité, nous utiliserons deux angles d'approche, soit d'un point de vue spécifique et d'un point de vue général.

D'un point de vue spécifique, l'identité a un caractère très unique et individuel (Clarke, 1994; Newman, 2008; Rannenberg, 2009; Saunders & Zucker, 1998, p. 185). Elle permet, entre autres, à une personne d'être reconnue et distinguée des autres. Dans cette approche plus psychologique, l'identité peut être définie à l'aide des éléments qui la structurent (Rannenberg, 2009, p. 39). Ainsi, elle est composée d'un ensemble d'attributs caractérisant une personne (Jones & Levi,

[17] Les travaux de l'association européenne *Future of Identity in the Information Society* (FIDIS) sont particulièrement pertinents sur la question de l'identité dans une société de l'information.

2000). Tout d'abord, dès la naissance, une personne possède des attributs biologiques (ADN, rétine, empreinte) qui lui sont uniques. Par la suite, une autorité reconnue émettra un extrait de naissance qui établit l'identité administrative (nom, date de naissance, nom des parents, lieu de naissance). Après, tout au long de la vie, l'individu se bâtira une identité biographique propre à ses échanges avec les autorités publiques, académiques, commerciales et professionnelles. Chaque organisation produira une série de documents plus ou moins officiels tels que le numéro d'assurance sociale, le numéro d'assurance maladie, le code permanent, le numéro d'employé, le numéro de client. Cette histoire de vie est relativement unique à chaque personne.

Ensuite, d'un point de vue général, l'identité peut être considérée comme un tout plus ou moins cohérent et uni. La littérature sur le sujet s'entend sur le fait qu'une personne possède plusieurs identités différentes en fonction des contextes, qu'il s'agisse de la vie sociale, professionnelle ou familiale (Rannenberg, 2009). En fait, l'identité est fragmentée et chaque entité avec laquelle le citoyen interagit, possède une représentation plus ou moins fidèle de l'identité globale de la personne. Chacun, qu'il s'agisse des compagnies d'assurances, de crédit ou de téléphonie, du gouvernement, des services de santé, de l'employeur, de l'institution d'enseignement, des collègues, des amis ou de la famille, a accès à des pièces à la fois différentes et similaires de l'identité (Rannenberg, 2009, p. 37). Dans les faits, il est intéressant de remarquer que la majorité des informations personnelles est contrôlée par des institutions, et que les individus ont un contrôle très limité sur la manière dont ces renseignements sont protégés et utilisés (Rannenberg, 2009, p. 36). Dans ce contexte, il est d'autant plus primordial que les mécanismes de contrôle (légaux, technologiques et éducationnelles) renforcent les pratiques des organisations afin d'encadrer la collecte, la gestion, la manipulation et l'exploitation des renseignements personnels.

3.1.2. Les caractéristiques de la cible

Dans les délits d'appropriation, les caractéristiques de la cible jouent un rôle essentiel dans la configuration de l'opportunité criminelle (Cusson, 1986, p. 15). Dans notre étude, on remarque que les données personnelles ont des caractéristiques intrinsèques qui les rendent attrayantes au vol. En effet, la recherche de Newman (Newman, 2008, pp. 13-14) montre que la notion de *hot product* développée par Clarke (1999), permettant d'identifier six attributs qui rendent un bien intéressant à voler, s'applique efficacement aux renseignements personnels.

Tout d'abord, les renseignements personnels constituent une cible accessible, car plusieurs organisations collectent et traitent des renseignements personnels. Comme nous l'avons mentionné, l'identité est morcelée et de plus en plus de personnes ont accès à des banques de données contenant des renseignements personnels dans le cadre de leur travail. Ainsi, la collecte systématique de renseignements personnels par les organisations a engendré une multiplication des cibles potentielles. Comme le mentionne Cusson (Cusson, 1986, p. 15), il est fort possible que l'augmentation du nombre de cibles fasse en sorte que de plus en plus de personnes ont l'opportunité de les voler.

Ensuite, les renseignements personnels sont une cible dissimulable. Ils peuvent être volés sans que la victime ou l'organisation le réalise. Les renseignements peuvent être volés physiquement ou ils peuvent être volés par un simple coup d'œil. L'information constitue également un bien facilement déplaçable. Cet élément est d'autant plus intéressant qu'avec l'univers numérique, des renseignements personnels de milliers d'individus peuvent être transportés sur une clé USB ou télécharger par Internet.

Par la suite, les renseignements personnels représentent un potentiel financier intéressant. Un voleur pourra convertir l'information volée en argent liquide par des achats en ligne, des demandes de crédit ou simplement en revendant l'information à un tiers. Newman (2008, p. 14) affirme également que pour un criminel, le vol de renseignements et la fraude sont des activités agréables qui leur procurent du plaisir. À ce sujet, la littérature sur les pirates informatiques démontre le plaisir que ces derniers ont à s'introduire dans les systèmes et le défi personnel qu'ils y trouvent. Dans le même ordre d'idées, Copes et Vieraiti (2007) affirment que les voleurs d'identité éprouvent un fort plaisir lorsqu'ils parviennent à voler et à convertir l'information en argent. Lors de leurs délits, les fraudeurs peuvent également éprouver du plaisir à manipuler leur victime.

Finalement, l'information constitue une cible vulnérable dans la mesure où la vulnérabilité peut se définir simplement par l'absence de risque pour le délinquant potentiel (Cusson & Cordeau, 1994). Selon Cusson (1986, p. 19), une cible est vulnérable quand le danger d'être arrêté, emprisonné, blessé ou tué que l'on court en tentant de se l'approprier est relativement bas. En fait, les gains qui découlent du vol d'information sont considérables et les risques d'être repéré, poursuivi en justice et puni sont relativement faibles. Bien que les sanctions pour le vol d'identité

semblent de plus en plus sévères et probables, il n'en demeure pas moins que ce type de criminalité n'est pas une priorité pour les organisations policières. Bref, il semble que plusieurs éléments, dont les caractéristiques de la cible, la multiplication de celle-ci et des déficits de protection, auraient stimulé de nouvelles opportunités criminelles que les délinquants motivés par l'appât du gain auraient vite fait de remarquer et d'exploiter.

3.1.3. L'ampleur des pertes d'information en Amérique du Nord

Au Canada, les données sur les pertes d'informations personnelles sont très parcellaires, car contrairement aux États-Unis, le Canada ne possède pas d'obligation légale de divulgation des brèches de sécurité entraînant la perte de renseignements personnels[18]. Par conséquent, très peu d'information est disponible sur le sujet et il existe peu de recherches scientifiques sur la compréhension, la tendance et l'ampleur du phénomène de vol de renseignements personnels. Les données les plus fiables sont celles collectées par le *data base loss*. Le tableau 1 présente l'évolution des brèches de sécurité qui ont entraîné la perte de renseignements personnels entre 2003 et 2010.

Tableau 1 : Les pertes de renseignements personnels aux États-Unis entre 2003 et 2010

	Nombre d'incidents	Variation avec l'année précédente (%)	Nombres de dossiers impliqués	Variation avec l'année précédente (%)
2003	13		7 055 450	
2004	23	76,9	2 317 590	-67,2
2005	141	513,0	55 988 256	2315,8
2006	537	280,9	51 251 706	-8,5
2007	511	-4,8	165 262 288	222,5
2008	787	54,0	86 930 805	-47,4
2009	604	-23,3	221 635 998	155,0
2010	407	-32,6	26 006 124	-88,3
Total	3 023		616 448 217	
Nombre moyen par année	378	123,4	75 957 717	354,5

[18] Selon le *National conference of states legislature*, seulement Alabama, Kentucky, Mississippi, Nouveau-Mexique et Dakota du Sud, n'ont pas de lois obligeant la divulgation de brèches de sécurité.

Selon cette organisation américaine qui récolte systématiquement toutes les pertes ou les vols de renseignements personnels[19], le nombre d'incidents a quadruplé entre 2005 et 2009, passant de 141 à 604. En 2008, un sommet de 787 incidents a été signalé pour un total de 86 930 805 dossiers compromis. Depuis 2003, 2 952 brèches de sécurité ont entraîné la divulgation non autorisée de 607 661 739 dossiers contenant des renseignements personnels. Au cours de ces huit années, 3 023 organisations ont été impliquées dans au moins un incident. 49% des incidents proviennent du secteur commercial, 20% de l'éducation, 17% des institutions gouvernementales et 14% du secteur de la santé. D'autres auteurs, dont Dupont et Louis (2009) ont eux aussi montré, en analysant 976 incidents de pertes ou de vols de données, ayant donné lieu à la compromission de 313 millions de dossiers personnels, que tous les secteurs d'activités semblent être victimes de défaillance en matière de protection des données personnelles.

Dans le même ordre d'idées, une étude, réalisée en 2009 par Rotman School of Business de l'Université de Toronto et TELUS à l'aide d'un questionnaire distribué auprès de 600 responsables de la sécurité informatique à travers le Canada, a démontré que tous les secteurs d'activités sont victimes de brèches de sécurité en matière de protection de l'information (Rotman & Telus, 2009). Les répondants qui provenaient des secteurs publics, privés et gouvernementaux, ont divulgué volontairement des détails sur leurs brèches de sécurité détectées. Les résultats du sondage démontrent une augmentation du nombre de brèches est passé de 9,6 incidents en 2008 à 34,1 en 2009. En plus de noter une augmentation globale du nombre de brèches par rapport à l'étude de l'année précédente, elle révèle que les organisations publiques sont le secteur qui connaît l'augmentation la plus marquée[20].

3.2. L'agent, gardien responsable de la protection des renseignements personnels

Le deuxième élément que nous devons prendre en considération lorsque l'on analyse une opportunité est le travail du gardien. Nous présenterons la littérature pertinente sur le rôle du gardien en deux temps. Dans un premier temps, considérant les centres d'appel comme le lieu d'interaction entre les présumés fraudeurs et le gardien, il nous semble indispensable d'aborder l'environnement de travail des agents afin de bien saisir sa complexité. Dans un deuxième temps,

[19] Contrairement aux États-Unis où la grande majorité des États ont adopté, depuis 2002, une obligation de divulgation des brèches de sécurité, le Canada ne possède pas ce type de législation.

[20] Les organisations gouvernementales ont été victimes en moyenne de 13.5 brèches en 2009 comparativement à 3.5 en 2008 pour des pertes évaluées à 1 004 799 $.

nous présenterons les vulnérabilités du processus décisionnel et du traitement de l'information chez l'agent.

3.2.1. La sociologie des centres d'appel

Pour les organisations, la protection des renseignements personnels, et dans un cadre plus large, la sécurité de l'information (SI), est un enjeu complexe qui implique à la fois des notions technologiques, humaines et organisationnelles. Pour cette recherche, nous présenterons l'enjeu de la protection des renseignements personnels dans un environnement bien particulier, celui des centres d'appel. La sécurité de l'information a rarement été abordée dans le contexte organisationnel des centres d'appel bien qu'il s'agisse d'un mode de gestion de plus en plus répandu.

Employant des millions de personnes à travers le monde, les centres d'appel sont un moyen de gestion largement répandu autant dans le secteur privé que public. Fondés sur une alliance du téléphone et de l'informatique, ils incarnent une modernité technologique accessible à tous en tout point du territoire (Buscatto, 2002, p. 100). Pour une organisation, les centres d'appel permettent d'offrir une variété de service, notamment de l'assistance ou de l'information, à un seul endroit sans que les clients aient besoin de se déplacer. Ils sont généralement un outil de rationalisation des dépenses en ressources humaines fortement axé sur la performance. Depuis quelques années, cette rationalisation des dépenses se traduit par une tendance dans l'industrie à la délocalisation des emplois à l'étranger où le coût des ressources humaines est très bas.

Il ne fait aucun doute que les employés des centres d'appel effectuent un travail très particulier. Dans une journée, les agents répondent à de nombreux appels similaires et de très courte durée avec des inconnus qu'ils ne rencontreront jamais (Taylor & Bain, 1999, p. 115). À chaque nouvel appel, l'agent doit se concentrer pour comprendre la demande du client, il doit visualiser plusieurs écrans à la fois pour trouver l'information au dossier et s'assurer de fournir la bonne réponse au client avec politesse. Aussitôt la conversation terminée et une nouvelle débute. Parfois les demandes sont très diversifiées et l'attitude du client varie à chaque appel. De plus, pour des besoins d'évaluation, d'assurance de qualité ou de formation, il arrive que les appels soient enregistrés. Ainsi, chaque conversation peut faire l'objet d'une évaluation. Sachant que son travail est continuellement mesuré, l'agent vit une pression qui le laisse épuisé mentalement, physiquement et émotionnellement (Taylor & Bain, 1999, p. 115). Enfin, dans les centres

d'appel, les salaires sont relativement bas et les possibilités de promotion sont limitées pour les agents (Taylor & Bain, 1999, p. 110). Toutes ces caractéristiques font en sorte que les centres d'appel doivent composer avec un haut taux de roulement de personnel.

Dans les années 1990, les centres d'appel ont été un terrain de recherche extrêmement riche pour le développement de la gestion scientifique (Aksin, Armony, & Mehrotra, 2007; Bain, Watson, Mulvey, Taylor, & Gall, 2002; Taylor & Bain, 1999). Se basant sur les principes de l'ingénieur américain Frederick W. Taylor (1856-1915), les gestionnaires des centres d'appel ont adapté leur environnement de manière à maximiser le rendement de l'organisation (Bain et al., 2002, p. 171). Taylor désirait diminuer le gaspillage des ressources et, selon lui, une gestion scientifique de l'organisation permettrait cette révolution (Bertrand, 1991, p. 12). Concrètement, les principes de Taylor visent une augmentation de la productivité par une division structurée du travail, une évaluation constante des processus, une surveillance des opérations, le développement de mesures de performance et l'évaluation de l'atteinte des objectifs.

Au sein des centres d'appel, les concepts d'évaluation et de surveillance sont très présents. Pour les gestionnaires, l'évaluation de la productivité de l'organisation revient inévitablement à l'atteinte d'objectifs quantitatifs, tel que le nombre d'appels traités et la durée de chaque appel, mais aussi à l'évaluation de la qualité du service offert (Bain et al., 2002, p. 172). La qualité du service à la clientèle peut être évaluée selon la convivialité, l'efficacité de la réponse fournie, la qualité du conseil et la satisfaction du client. Considérant que les centres d'appel sont une organisation de service à la clientèle (Bain et al., 2002, p. 173), il est indispensable pour les gestionnaires de trouver un équilibre fragile entre l'atteinte des objectifs quantitatifs et qualitatifs.

Cependant, à l'intérieur de l'organisation, cette rationalisation extrême de la relation de service téléphonique crée des tensions entre les gestionnaires et les employés (Buscatto, 2002). Pour les gestionnaires, la gestion du personnel est complexe et les pressions du marché sont très fortes. Afin de se démarquer, les organisations doivent à la fois valoriser la quantité et la qualité (Taylor & Bain, 1999, p. 110). Ainsi, les gestionnaires désirent atteindre des cibles quantitatives, mais ils insistent également sur l'importance de la qualité du service à la clientèle visant à offrir une valeur ajoutée afin de se démarquer sur le marché. Cependant, les caractéristiques du travail font en sorte que les employés sont démotivés et épuisés. Par conséquent, ils sont moins sensibles

à la demande du client ce qui nuit à la fois à la productivité, à la sécurité et à la qualité du service à la clientèle.

Si les partisans du Taylorisme argumentent que les centres d'appel représentent le nouveau développement du travail du col blanc selon des principes reconnus d'efficacité (Taylor & Bain, 1999, p. 115), plusieurs soulèvent qu'il se cache derrière ces concepts, une réalité sombre caractérisée par le stress, la pression, la productivité et un travail pénible. En effet pour certains, les centres d'appel sont une image moderne du travail des ouvriers des usines qui était, au début du 20^{e} siècle, déshumanisé par les objectifs de productivité.

Certains auteurs présentent les centres d'appel comme l'intégration moderne du panopticon de Bentham (Fernie & Metcalf, 1998; Knights & McCabe, 1998). Le panopticon est le célèbre dispositif de contrôle élaboré par le philosophe anglais Jeremy Bentham (1791) à la fin du 18^{e} siècle. Ce système consiste à ériger une tour au centre d'une prison afin qu'un gardien ait la possibilité de surveiller tous les prisonniers, mais sans que ceux-ci sachent s'ils sont surveillés. Ce modèle de contrôle agit sur la conscience en créant un sentiment de surveillance omniprésent, mais invisible. Depuis plusieurs années, les travaux sur la vidéo-surveillance (voir Gordon, 1987; Leman-Langlois, 2002; Norris & Armstrong, 1999) ont adopté cette métaphore du panopticon pour expliquer l'effet des caméras sur le comportement des gens.

En ce qui a trait à l'application de ce concept dans l'environnement des centres d'appel, il provient d'une comparaison empruntée des travaux Foucault (1975) sur l'omniprésence de la surveillance dans la société. Selon Foucault (1975), la surveillance est une forme de pouvoir disciplinaire, très présente dans les institutions, et elle constitue une caractéristique fondamentale de l'application du contrôle social moderne. Un individu, ne sachant pas s'il est surveillé ou non, supposera qu'il l'est toujours et agira en conséquence. Dans les centres d'appel, les analyses de Foucault ont attiré l'attention en raison de l'importance accordée à l'évaluation. En effet, dans les centres d'appel, chaque action peut être surveillée électroniquement et faire l'objet d'une évaluation précise. Cette fonction de contrôle semble faire partie intégrante de la philosophie de l'organisation de tous les centres d'appel. Fernie & Metcalf (1998) avancent que cette surveillance permanente donne aux gestionnaires un contrôle ultime et total. Ce panoptique électronique est un puissant mécanisme de contrôle informel et non coercitif qui oblige les employés à se conformer aux attentes de l'environnement.

Selon Taylor et Bain (1999, p. 116), les preuves empiriques ne démontrent pas qu'il est possible d'appliquer le panoptique de Bentham d'une manière aussi pessimiste que Fernie et Metcalf (1998) le voudraient. Bien qu'ils ne contestent pas l'existence d'un panoptique électronique dans les centres d'appel, Bain et Taylor (2000, pp. 16-17) disent que l'application de ce concept est superficielle et inexacte, car elle oublie une multitude de facteurs tels que la complexité de la gestion et elle ne tient pas compte que les agents sont des acteurs actifs et non passifs par rapport à cette surveillance. Par contre, ils ne nient pas qu'il s'agisse d'un environnement stressant, répétitif, intense, exigeant psychologiquement et que le travail est mesuré plus que n'importe où ailleurs. Un sondage du *Communication Workers of America* confirme que la surveillance électronique est la principale source de stress et qu'elle crée un sentiment de dépression et d'anxiété (cité dans Taylor et Bain, 1999, p. 114). Selon Bain, et al. (2002, p. 173), l'organisation du travail dans les centres d'appel n'est pas une application sombre du Taylorisme mais plutôt une évolution significative adaptée au 21^{e} siècle.

3.2.2. La sécurité de l'information et les centres d'appel

Comme tous les environnements organisationnels, les centres d'appel sont un système de règles plus ou moins cohérent qui doit faire face à divers dilemmes et contradictions afin d'atteindre leurs objectifs. Ces différentes logiques doivent coexister et alors que certaines se complètent, d'autres se nuisent ou même s'opposent. En matière de sécurité, les incohérences, entre les logiques de productivité, d'efficacité, de service à la clientèle et de sécurité, représentent des failles exploitables par les délinquants, car elles placent les employés dans des situations ambivalentes (Moir & Weir, 2008, p. 23). Placé dans des situations inconfortables, l'agent des centres d'appel doit prendre des décisions, qui consciemment ou inconsciemment, peuvent menacer l'intégrité de l'information.

Ainsi, dans les centres d'appel, les vulnérabilités qui facilitent la perte d'information seraient à la fois individuelles et organisationnelles. Selon les résultats d'une recherche de Kraemer, Carayon, et Clem (2009), les facteurs humains et organisationnels sont interreliés et ils jouent un rôle déterminant dans le développement de faille en matière de sécurité de l'information. Pour notre étude, l'identification et la compréhension de ces vulnérabilités sont essentielles, car elles structurent l'opportunité de vol de renseignements personnels.

Il importe de préciser que lorsque nous parlons de vulnérabilité, nous ne nous intéressons pas à l'erreur humaine d'un point de vue individuel, mais aux dynamiques et au contexte de travail favorisant des comportements qui peuvent compromettre la sécurité de l'information. À l'instar de différentes recherches (Kraemer et al., 2009; Werlinger, Hawkey, & Beznosov, 2009), nous diviserons les facteurs en deux groupes, soit organisationnels et individuels.

3.2.3. Les facteurs organisationnels

3.2.3.1. Les motivations et l'engagement

Comme nous l'avons mentionné, plusieurs centres d'appel enregistrent les conversations afin d'évaluer la qualité du service, le temps de chacun des appels ainsi que le temps passé hors ligne. Selon Taylor et Bain (1999, p. 116), cette évaluation constante peut avoir un impact négatif important sur la motivation et l'engagement des employés. Ainsi, une surveillance intensive du travail des agents peut engendrer des résultats contre-productifs. En matière de sécurité, un employé qui n'est pas motivé risque de porter moins attention aux gestes qu'il pose et aux menaces auxquelles il fait face. De plus, en règle générale, les employés ont de la difficulté à adhérer aux mesures de sécurité, car elles nuisent à leur travail quotidien. Pour plusieurs organisations, il est d'autant plus difficile de motiver les employés à respecter les mesures de sécurité que la pression à appliquer les normes provient de d'autres départements ou d'organisations qui n'ont aucun lien avec les centres d'appel.

3.2.3.2. L'ambivalence du rôle

Il existe, dans les centres d'appel, diverses contradictions organisationnelles qui placent les employés dans des situations ambivalentes. Si le premier dilemme entre la quantité et la qualité est fortement documenté (Bain et al., 2002; Taylor & Bain, 1999), le second entre la sécurité, le service à la clientèle et la productivité est relativement peu abordé dans les recherches scientifiques.

Tout d'abord, considérant que les centres d'appel sont fortement axés sur la productivité de leurs employés, Taylor & Bain (1999) et Moir & Weir (2008) soulèvent le dilemme profond entre la quantité et la qualité. Ce problème est inhérent à tous les centres d'appel et il est d'autant plus complexe qu'aujourd'hui les organisations accordent une place importante à la qualité du service rendu au client, mais tout en gardant des cibles très élevées au niveau de la productivité. Ainsi, il

peut arriver que l'impératif de productivité fasse en sorte qu'une conversation qui s'éternise fera perdre du temps à l'employé et que la tentation de céder aux demandes de l'usager pour passer à l'appel suivant soit forte. Afin de préserver de bonnes statistiques, l'agent répondra le plus rapidement possible à la demande de la personne.

Une deuxième source de tension provient du dilemme entre offrir un service de qualité à la clientèle et appliquer les mesures de sécurité. Dans un centre d'appel, la principale mesure de sécurité consiste à appliquer un protocole d'identification. Lorsqu'un citoyen appelle une organisation, il doit répondre correctement à une série de questions afin de prouver son identité au risque de se voir refuser la divulgation de renseignements à son dossier. Pour certains clients, ce protocole d'identification est irritant, car en plus de ne pas saisir la nécessité de ces questions, ils doivent aller chercher des documents et répondre à des questions qui sont parfois personnelles. Ainsi, le protocole crée une certaine friction entre le client et l'agent. Cette friction est d'autant plus difficile à éliminer que le protocole est la première chose demandée au client, car l'agent doit confirmer l'identité de la personne avant de communiquer tout renseignement.

Dans la mesure où le client échoue le protocole d'identification ou si l'agent a de bonnes raisons de croire que l'usager n'est pas la personne qu'il prêtant être, l'agent doit rester convivial et lui refuser l'accès. Pour un agent, ces deux objectifs peuvent être en profonde contradiction, car les personnes qui travaillent dans les centres d'appel font généralement ce travail parce qu'elles aiment offrir un service à la clientèle de qualité et répondre aux besoins des personnes. Or, à chaque appel, l'agent doit appliquer le protocole d'identification et cela peut causer des frictions avec le client. C'est précisément cette situation ambivalente qu'exploitent les fraudeurs (Moir & Weir, 2008, p. 3). Conscient que la priorité n'est pas toujours la sécurité, les présumés fraudeurs utilisent la notion de bon service comme levier afin de placer l'agent dans une situation inconfortable. Ils créeront une multitude de prétextes afin de mettre de la pression sur l'agent pour que ce dernier cède à sa demande.

Si l'application du protocole peut nuire d'une certaine manière à la qualité du service offert par l'organisme public, elle entre également en conflit avec les concepts de productivité et d'efficacité. L'application d'un protocole d'identification standard, c'est-à-dire la confirmation de trois identifiants personnels, prend à elle seule de 30 à 90 secondes. Par la suite, l'agent doit bien saisir la question du client, trouver la réponse, lui communiquer et s'assurer que le client n'a

pas d'autres questions. Le protocole d'identification demande beaucoup de temps et il est le seul élément sur lequel les agents ont le contrôle. Ainsi, un agent peut vouloir diminuer son temps d'appel en posant les questions les plus simples et les plus rapides.

3.2.4. La culture de sécurité

La culture organisationnelle est la perception et l'interprétation des valeurs d'une organisation que se donnent ses membres afin d'être en mesure de comprendre, d'apprendre et d'agir (Bertrand, 1991, p. 7). Développé dans les années 1960 et inspiré des travaux de F. W. Taylor sur le besoin de révolution dans la gestion des organisations, le concept de culture organisationnelle est à la fois une description de ce qu'est l'organisation et une illustration idéale de ce qu'elle désire être. Il s'agit d'un concept global hautement politique qui permet, entre autres, de mobiliser les énergies et les focaliser sur quelques objectifs majeurs, de canaliser les comportements autour d'un certain nombre de normes d'action, de freiner ou d'accélérer le changement, d'encourager la loyauté envers l'organisation et de mobiliser le personnel (Bertrand, 1991, p. 55).

Dans une organisation, il est possible de créer une culture de sécurité au même titre que n'importe quelle autre valeur (Knapp, Marshall, Rainer, & Ford, 2006, p. 33). La culture de sécurité est un moyen de protection relativement efficace, car il s'agit d'un outil de contrôle, de mobilisation et d'influence informel particulièrement puissant. Cependant, en pratique, il s'agit d'un concept difficile à opérationnaliser et son application peut impliquer que l'organisation fasse des concessions sur d'autres dimensions telles la compétitivité ou la capacité de réagir aux changements de l'environnement. La littérature sur la sécurité de l'information permet de retenir certains éléments clés. Pour une organisation, l'absence d'une culture de sécurité et de ses composantes représente des vulnérabilités qui augmentent le risque de perte d'information.

En effet, des recherches empiriques ont montré que le support de la haute direction était significativement associé à une culture de sécurité et au niveau d'implication des employés (Knapp et al., 2006, p. 34). Outre l'implication de la direction, l'organisation doit considérer la gestion et la coordination de la sécurité comme un processus vivant (Knapp et al., 2006, p. 33). C'est-à-dire que la sécurité doit être intégrée dans les opérations quotidiennes et qu'elle doit faire l'objet d'un suivi, d'une évaluation et de modifications constantes.

Concrètement, une organisation doit mettre en place des politiques et procédures (Kraemer et al., 2009, p. 518) et allouer des ressources humaines. De plus, elle doit faire de la sensibilisation afin que les employés soient informés, et dans un monde idéal engagé envers la mission de sécurité (Siponen, 2000, p. 39). Cependant, comme le souligne Albrechtsen (2007, p. 288), la sensibilisation ne doit pas être effectuée en masse, mais plutôt de manière ciblée et adaptée à un groupe précis si l'on veut influencer les comportements. Idéalement, la sensibilisation doit être accompagnée de la formation afin de limiter les comportements dangereux (Kraemer et al., 2009, p. 518; Stanton, Stam, Mastrangelo, & Jolton, 2005). La formation peut être efficace, car Stanton et al. (2005) ont démontré, dans une recherche sur l'utilisation de mot de passe, qu'elle permettait, dans une certaine mesure, de modifier les comportements. Évidemment, la ligne distinguant les facteurs organisationnels et individuels n'est pas clairement définie. Il ne fait aucun doute que les deux concepts se chevauchent et qu'ils s'influencent mutuellement. Ainsi, l'action individuelle est influencée par l'environnement et l'environnement est la somme des individus qui le composent.

3.2.5. L'élément humain de la sécurité de l'information

La littérature concernant la sécurité de l'information est largement dominée par des écrits techniques qui visent la conception de modèle informatique sécuritaire, l'investigation de brèches de sécurité et l'évaluation des mesures technologiques en place (Jamieson et al., 2008, p. 444). Lors des dernières années, différents standards, notamment ISO 27002, ont été développés afin de fournir aux organisations un ensemble de pratiques de gestion reconnu permettant d'assurer une meilleure protection de l'information. En matière de sécurité de l'information, les solutions technologiques se sont avérées un choix logique et efficace notamment en raison des progrès impressionnants qui ont été effectués dans le domaine de la cryptographie, de la détection des intrusions, des antivirus, des pare-feu et d'autres équipements de sécurité informatique (Sarriegi, Santos, Torres, Imizcoz, & Plandolit, 2006, p. 3). Il n'est donc pas surprenant que la protection de l'information soit largement considérée comme une responsabilité informatique (Besnard & Arief, 2004; Kraemer et al., 2009, p. 509).

Cependant, ce constat ne fait pas l'unanimité. En effet, plusieurs recherches récentes montrent que les solutions technologiques ont d'importantes limites, car elles négligent considérablement l'importance de l'élément humain dans la chaîne de protection (Werlinger et al., 2009, p. 5). En

fait, toute une littérature en informatique argumente qu'il est impératif de revoir l'attention accordée à l'élément humain dans la protection de l'information. Selon ce courant, l'humain doit être considéré à la fois comme l'élément le plus vulnérable d'un système de sécurité et la partie maîtresse dans la protection de l'information (Carr, 2009; Dontamsetti & Narayanan, 2009; Mann, 2008; Nohlberg, 2009b; West, Mayhorn, Hardee, & Mendel, 2009). Ces auteurs notent également que peu importe le niveau de sophistication et de complexité d'un système de sécurité, l'individu ayant légitimement accès demeure l'élément le plus vulnérable.

Deux raisons expliquent pourquoi l'humain est l'élément faible de la chaîne de sécurité. Tout d'abord, il commet plusieurs erreurs dans sa prise de décision. Ensuite, la personne ayant légitimement accès à l'information est vulnérable, car elle peut être manipulable et amener consciemment ou non à divulguer de l'information confidentielle. L'ingénierie sociale, qui est l'art d'utiliser la tromperie et le mensonge pour arriver à ses fins (Mitnick & Simon, 2003, p. 41), exploite précisément ce maillon faible de la chaîne de sécurité afin d'avoir accès à l'information confidentielle. Ainsi, il semble que la forme de la menace et les solutions à la protection de l'information ne résident pas dans la sphère technologique. Schneier (2008) semble viser juste lorsqu'il dit que les gens qui croient résoudre un problème de sécurité avec de la technologie n'ont rien compris aux problèmes, ni à la technologie. Faisant à la fois partie de la solution et du problème, il est essentiel de s'attarder au processus décisionnel qui guide les actions humaines.

3.2.6. Les facteurs individuels

Afin de comprendre comment les humains prennent leurs décisions, nous avons utilisé les recherches en psychologie cognitive qui étudient comment les individus perçoivent, apprennent, se souviennent et pensent l'information qu'ils reçoivent (Launay & Benedetto, 2004, p. 13). Comme nous le verrons, ces enseignements nous apportent d'importantes précisions sur le processus décisionnel de l'humain et ses impacts sur la protection de l'information.

3.2.6.1. La prise de décision en sécurité

Pour débuter, devant une situation complexe, il est très rare qu'une personne possède toutes les informations nécessaires afin de prendre la décision optimale. On peut donc dire que la capacité de raisonnement est, entre autres, limitée aux informations connues par la personne. Ce concept développé par Herbert Simon (1957) signifie que lors d'une prise de décision, pour diverses raisons, une personne ne peut pas considérer toutes les options et que par conséquent, elle

choisira la première option satisfaisante qui se présentera à elle au moment de la décision et non la solution la plus optimale. Pour choisir l'option la plus satisfaisante, elle devrait prendre connaissance de toutes les options qui se présentent à elle et de leurs avantages réciproques, ce qu'elle n'a pas le temps et les capacités mentales de faire.

Il est pertinent d'ajouter le postulat de la rationalité, c'est-à-dire que placé devant une décision, l'humain cherche à maximiser ses gains et à réduire ses pertes. Cependant, comme le souligne West et al. (2009) pour un agent des centres d'appel, la prise de décision impliquant la divulgation ou non de renseignements personnels, résulte d'un calcul coûts-bénéfices difficilement opérable mentalement. En effet, la sécurité est un concept abstrait et subjectif intimement lié à une action dans un espace de temps donné. Ainsi, les gains et les conséquences d'une action sécuritaire sont difficiles à évaluer. Par exemple, les bénéfices sont souvent sous-évalués alors que les coûts surévalués, ce qui crée un environnement pour une prise de décision déficiente. Devant quotidiennement prendre des décisions qui impliquent une certaine notion de sécurité, le processus décisionnel de l'humain tient davantage de l'intuition[21] que de la logique. Par contre, ce qui est impressionnant, c'est que la psychologie cognitive a démontré que même si un individu possédait toute l'information nécessaire pour prendre la bonne décision, il prendrait celle grandement inférieure à la solution optimale (Tversky & Kahneman, 1974). En effet, lorsqu'une décision implique un nombre élevé de variables, les recherches en psychologie cognitive ont démontré que le cerveau humain semble mal adapté à des raisonnements complexes.

L'une des explications de ces erreurs de jugement serait l'utilisation de raccourcis mentaux, appelés heuristiques, lors du traitement de l'information. Les heuristiques sont utilisées quotidiennement, car elles sont hautement économiques en temps et en énergie. Elles permettent à l'humain de prendre des décisions rapide et efficace. Notre environnement est rempli de stimuli extrêmement divers et il nous est impossible d'analyser chacun des éléments qui composent chaque situation. Le temps, l'énergie et les capacités nous manquent (Cialdini, 1993, p. 16). À défaut, nous avons recours aux heuristiques qui sont fortement basées sur l'impression qui

[21] En effet, les recherches en psychologie ont montré que l'humain est une espèce très intuitive. Lorsqu'il traite de l'information, il arrive fréquemment que le cerveau saute à des conclusions et qu'il prenne des décisions presque instantanément.

survient automatiquement et indépendamment de toute évaluation objective de la situation pour prendre des décisions rapidement.

Ainsi, lorsque l'on observe le même produit provenant de différentes compagnies informatiques, il nous semble normal de croire que celui dont la valeur est supérieure soit de meilleure qualité. Ces automatismes permettent de prendre une décision rapidement et ils sont efficaces dans la très grande majorité des cas. Car normalement, le prix d'un article est proportionnel à sa valeur; un prix élevé est généralement l'indice d'une qualité élevée (Cialdini, 1993, p. 15). Cependant, ces biais de raisonnement représentent une vulnérabilité, car ils entraînent des déviations systématiques et prévisibles qui peuvent être facilement exploitées par quelqu'un qui est conscient de ces faiblesses. Les heuristiques sont à différencier de l'erreur qui est aléatoire, alors que les biais de raisonnement présentent un certain déterminisme. En d'autres mots, les heuristiques entrainent une décision erronée qu'il est possible de prédire. Quant à l'erreur, elle peut être le fruit de distraction, de fatigue, d'insouciance ou d'oubli qui est impossible à prédire.

3.2.6.2. La perception du risque

La perception du risque ne représente pas une donnée objective, mais plutôt une construction subjective influencée par les connaissances, l'expérience et les stimulus de l'environnement (Rosa, 2003; Slovic, Finucane, Peters, & MacGregor, 2004; Workman, 2008b). S'il est possible d'évaluer objectivement le risque à l'aide de calcul élaboré dans certains domaines, elle n'est que très rarement utilisée car elle est fastidieuse et exigeante mentalement. En fait, l'humain comprend avant tout le risque comme un sentiment qui apparaît intuitivement voire presque automatiquement et inconsciemment devant une situation (Slovic et al., 2004). Selon les études de Slovic (1975, 1987; 1980), cette perception subjective du risque diverge grandement de toute évaluation objective et les heuristiques, présentées précédemment, expliqueraient en partie la divergence de perception entre le risque objectif et subjectif. Dans la présente recherche, il est pertinent de s'attarder à la manière dont les agents perçoivent le risque lié aux tentatives non autorisées d'obtention de renseignements personnels car les études indiquent qu'ils baseront leur évaluation d'une situation avant tout sur un calcul subjectif. Ainsi, il est probable que cette perception diverge d'une compréhension objective et élaborée de la situation.

De plus, les recherches sur la perception des risques (Pyszczynski, Greenberg, & Solomon, 1997; Slovic, 2000) indiquent qu'une personne ajuste son comportement en fonction de sa perception du risque. Considérant le risque faible, une personne ne procédera pas au traitement de l'information de manière aussi rigoureuse que si elle considérait le risque élevé. Ainsi, la perception d'un événement ou d'un individu est un élément important, car elle influence l'attitude et le comportement d'une personne (Greenwald & Banaji, 1995; Sjöberg, 2000). Selon Workman (2008a, p. 466), une personne qui perçoit une menace comme faible agit moins prudemment. De plus, toujours selon cet auteur, les personnes qui se croient moins vulnérables à une attaque ont plus de chance de commettre des erreurs que ceux qui se considèrent plus vulnérables. Pour une organisation, la perception du risque des employés a un impact majeur sur le comportement que ceux-ci adopteront face à une situation. Lorsque le risque est sous-estimé, cela entraîne des comportements inadaptés, car les gens n'ont aucun intérêt à se protéger contre cet événement. Dans cette logique, la perception que les gens ont de la sécurité, du phénomène du vol de renseignements personnels ou d'un individu, influence leur comportement.

La psychologie cognitive a identifié différents biais dans le traitement de l'information qui peuvent expliquer pourquoi l'humain a une perception du risque qui s'éloigne d'un calcul objectif. Dans les prochaines lignes, nous aborderons certains biais qui altèrent la perception du risque et que nous jugeons pertinents dans le contexte de cette recherche. Tout d'abord, la perception du risque n'est pas représentative de la réalité car les gens surestiment la fréquence et les conséquences de plusieurs risques mineurs alors qu'ils négligent d'autres risques majeurs. Par exemple, ils exagèrent les risques spectaculaires, rares, populaires, immédiats, incertains, hors de notre contrôle, nouveaux et moralement dérangeants (Schneier, 2008, p. 6; Slovic, 1987)

Ensuite, l'humain a particulièrement de la difficulté à évaluer la probabilité qu'un événement survienne. L'origine de ce problème réside dans l'utilisation de l'heuristique de la disponibilité qui consiste à fonder les estimations sur la facilité de récupération en mémoire des exemples que l'on considère comme pertinents (Kahneman, Slovic, & Tversky, 1982). En fait, l'humain ne cherche pas d'autres informations que celles immédiatement disponibles. L'utilisation de cette heuristique peut amener l'individu à surestimer le poids des dimensions les plus rares de l'événement en raison de leur forte disponibilité en mémoire. Ce biais influence l'évaluation de la fréquence et de la probabilité d'événement. Bien évidemment, les occurrences récentes et les événements les plus marquants sont les plus disponibles.

Par la suite, les gens ont tendance à chercher et à sélectionner les informations qui confirment leur hypothèse de départ au détriment des informations qui prouvent qu'elle est fausse (Office of fair trading, 2009, p. 28). C'est-à-dire que l'humain a une préférence pour les éléments qui confirment les croyances passées. Il est sélectif dans le choix des informations si bien que les nouvelles informations seront jugées pertinentes et riches seulement si elles sont en accord avec les croyances passées (Frey, 1986). De l'autre côté, lorsqu'elles vont à l'encontre des croyances de la personne, elles seront considérées comme inintéressantes ou erronées. Ce biais réduit considérablement la qualité de la décision et altère la perception du risque, car de nouvelles informations pertinentes seront ignorées (Kray & Galinsky, 2003, p. 76). Ce biais de raisonnement, aussi connu sous le nom d'ancrage, peut devenir un outil d'influence important, car il est généralement facile de cibler les croyances d'une personne. Une fois la cible placée dans une situation où elle doit prendre une décision, le fraudeur lui donne toute sorte d'information qui confirme ses croyances et qui joue à son avantage.

Finalement, on considère, à tort, certains éléments spécifiques d'un individu comme représentatifs d'une population (Tversky & Kahneman, 1974). Cette heuristique consiste à estimer la probabilité d'un événement en fonction du degré de similarité avec la population d'où il est extrait. Par exemple, les avocats sont habituellement des personnes strictes, sérieuses et honnêtes. En fait, la personne construit son jugement en se fondant sur la ressemblance de la personne perçue à une personne connue. Un raisonnement semblable, mais négatif est également fréquent. Si une personne découvre que des réparations non nécessaires ont été effectuées sur son véhicule par un mécanicien, elle associera tous les mécaniciens comme des gens malhonnêtes. Ce lien de similarité est fortement nourri par les stéréotypes. Ainsi, les fraudeurs vont utiliser les stéréotypes à leur avantage pour influencer le jugement de la cible. Par exemple, un fraudeur cherchera à créer un lien de similarité en prétendant avoir déjà travaillé pour la même organisation que la cible ou avoir occupé un poste semblable.

D'autres biais sont également à l'origine d'une mauvaise évaluation du risque, notamment celui de l'excès de confiance. Selon une étude de Armor & Taylor (2002) et Alicke & Govorun (2005), les gens ont une image très positive d'eux-mêmes et ils surestiment leurs propres compétences et connaissances. Cette présomption par excès de confiance incite les individus à prendre de mauvaises décisions. Ensuite, on retrouve le biais de la détection du mensonge, c'est-à-dire que les gens surestiment presque toujours leur capacité à détecter le mensonge (Elaad, 2003; George

et al., 2004; Marett, Biros, & Knode, 2004). Ce biais devient encore plus problématique lorsque l'on considère le biais de vérité, c'est-à-dire que les gens sous-estiment la possibilité que quelqu'un mente (Martin, 2004). Ces deux biais expliquent, entre autres, pourquoi l'humain est vulnérable à la manipulation. Un autre élément à considérer est que les gens ont tendance à croire que les mauvaises choses telles que la mort, les désastres naturels, un crime, une fraude, un accident n'arrivent qu'aux autres (Armor & Taylor, 2002; Levine, 2003). Ce raisonnement, appelé le biais d'optimisme, peut aussi être transposé à une organisation qui ne prend pas au sérieux certains risques et se croit protégée de tout. Il s'agit d'une illusion d'invulnérabilité qui amène l'humain à se croire peu susceptible de subir des conséquences négatives.

Bref, dans le quotidien, en l'absence des informations appropriées et du temps pour effectuer une analyse complète, le calcul du risque est le résultat d'une évaluation subjective. Les études présentées montrent que le raisonnement de l'humain est altéré et que généralement, son évaluation du risque est erronée. Ces conclusions mettent en lumière l'importance pour une organisation de bien informer leurs employés de la nature des risques et des conséquences potentiels de leur action.

3.2.6.3. Le stress et la pression

Le stress est également un élément important qui peut affecter le processus décisionnel des agents lors des appels (Hammond, 2000). Dans un centre d'appel, le stress provient à la fois de l'environnement de travail et de l'appel. En effet, la pression constante afin d'être productif et la charge de travail sont des éléments stressants pour l'agent. À chaque appel, l'agent vit également des pressions de la part du client qui désire avoir accès à son dossier. Selon Hammond (2000), ces facteurs diminuent l'attention et la capacité de prendre la décision optimale. Donc, le niveau de stress vécu par les agents influence le traitement de l'information.

3.2.6.4. Les études de modèles intégrés

Quelques études ont développé des modèles complexes qui intégraient l'ensemble des facteurs de risque organisationnels et individuels. À l'aide de groupe de travail avec des responsables de la sécurité de l'information, Kraemer et al. (2009, p. 516) ont identifié les relations directes et indirectes entre quarante-quatre (44) facteurs humains et organisationnels. Pour leur part, Werlinger et al. (2009, p. 14) identifient à l'aide d'entretiens semi-directifs avec trente-six (36)

responsables de la sécurité de l'information, l'importance que chacun accorde aux dix-sept (17) facteurs de risque (organisationnels, humains et technologiques) qu'ils avaient préalablement identifiés. Ils décrivent, dans leur étude, les interrelations entre les facteurs humains, organisationnels et technologiques. Cependant, les auteurs ne quantifient pas le poids de ces relations. Quant à Sarriegi et al. (2006, pp. 9-10), ils élaborent un diagramme qui permet de mettre en relation les différents facteurs et d'évaluer le poids de chaque relation. Selon ces derniers, cinq éléments sont centraux soit la formation, la sensibilisation, les logiciels pour prévenir, l'analyse des risques (identifier les actifs prioritaires, les vulnérabilités, les menaces) et l'implantation de politiques et procédures (Sarriegi et al., 2006, p. 12). Bref, bien que les différentes études s'entendent sur tous les facteurs qui influencent la protection de l'information ainsi que l'importance de chacun, elles s'accordent pour dire qu'il existe une interrelation complexe entre les facteurs humains et organisationnels.

3.3. Le délinquant motivé

Dans la section précédente, nous avons identifié une série de vulnérabilités organisationnelles et humaines représentant un risque pour la sécurité de l'information. Cependant, la seule présence d'une vulnérabilité ne constitue pas un problème pour une organisation. Pour être un problème, la vulnérabilité doit être exploitée par une menace. Ainsi dans la prochaine section, nous dresserons le profil des personnes qui profitent de ces vulnérabilités afin d'obtenir de l'information confidentielle ainsi que leurs motivations. Enfin, nous présenterons plusieurs techniques utilisées par les fraudeurs.

3.3.1. Le profil

Le troisième et dernier élément composant l'opportunité est le délinquant motivé. Lorsque nous analysons le profil des délinquants, nous remarquons qu'il s'agit d'une forme de délinquance aux profils très hétérogènes. En effet, les femmes sont, entre autres, surreprésentées dans cette forme de criminalité comparativement à d'autres types de crime. Selon les résultats de l'étude de Gordon, Rebovich, Choo & Gordon (2007), 33% étaient des femmes. Arrivant à la même constatation, dans leur analyse du profil des voleurs d'identité, Dupont et Louis (2009) expliquent ce résultat par le fait que le vol d'identité n'est pas un crime violent et qu'il peut être exécuté individuellement.

Ensuite, environ 42,5% des accusés sont âgés de 25 à 34 ans (Gordon et al., 2007, p. 31). Dans un échantillon de 59 criminels reconnus coupables de vol d'identité, Copes et Vieraitis (2009) notent que 52,5% occupaient un emploi au moment de l'arrestation. En qualifiant leur situation financière, 47,5% disaient être dans la classe moyenne ou 42,4% dans la classe moyenne élevée. Toujours dans cet échantillon, 25% étaient mariés au moment du crime. Enfin, plus de 71% n'avaient pas d'antécédents criminels. Ce taux élevé de première arrestation pourrait être dû au fait que des gens ordinaires, sans antécédent, profitent de l'opportunité criminelle que représente le vol d'information afin de faire des profits rapidement. Ces résultats peuvent aussi être dus au fait que les délinquants plus expérimentés parviennent à se soustraire à la justice. En d'autres mots, il est possible que les organisations policières préfèrent concentrer leurs ressources sur les cas plus simples (Dupont & Louis, 2009).

3.3.2. Les motivations

Les informations quant aux motivations derrière le vol de renseignements personnels sont parcellaires notamment en raison du faible taux d'arrestation. Cependant, les études scientifiques s'accordent pour dire que les principales motivations derrière le vol de renseignements personnels sont économiques (Copes & Vieraitis, 2009, p. 245; Dupont & Louis, 2009, p. 13; Gordon et al., 2007; Gordon & Willox Jr, 2004; Newman & McNally, 2005; Synovate, 2007). Considérant que la principale source d'information pour cette criminalité provient de sondage de victimisation, il n'est pas surprenant que les données que l'on possède proviennent des personnes ayant subi des pertes financières. Le tableau 2, tiré de l'étude de Gordon et als (2007, p. 38), présente les principales motivations derrière le vol de renseignements personnels. Si la majorité des voleurs d'identité cherchent l'enrichissement immédiat, une portion de ceux-ci utilise l'information volée pour créer une identité synthétique[22] (22,7%), pour revendre l'information (7,7%) ou obtenir des services gouvernementaux illégalement (3,8%).

[22] Une identité synthétique est une identité fictive créée à partir d'un ensemble de renseignements authentiques et fabriqués. Le fraudeur peut utiliser un vrai NAS, avec un faux nom et adresse. En d'autres mots, ces identités ne correspondent pas à de vrais individus et sont rarement signalées aux services de police, car il n'y a pas de victime directe.

Tableau 2 : Les motivations derrière le vol d'identité

	(n)	(%)
	705	140*
Pour obtenir du crédit	228	45,3
Pour obtenir de l'argent liquide	166	33
Pour fabriquer et utiliser une fausse identité	114	22,7
Pour acheter un véhicule	105	20,9
Pour fabriquer et vendre une fausse identité	39	7,7
Pour obtenir des services téléphoniques	23	4,6
Pour obtenir des bénéfices de programmes gouvernementaux	19	3,8
Pour se procurer de la drogue	11	2,2

* Le pourcentage total est plus élevé que 100% car certains fraudeurs avaient plusieurs motivations au moment de l'arrestation.

Cependant, une partie non négligeable, mais difficilement quantifiable, des vols d'information sont utilisés afin de faciliter la demande de document officiel, l'immigration clandestine, l'accès illégal à des services gouvernementaux, pour éviter une arrestation ou pour le terrorisme (Dupont & Louis, 2009, p. 13; Sproule & Archer, 2006).

D'autres motivations peuvent également être attribuées aux vols de renseignements personnels. En effet, Hart (2010, p. 59) mentionne que les investigateurs privés, les journalistes d'enquêtes, les groupes criminels professionnels prétendent souvent être quelqu'un d'autre afin d'avoir accès à des renseignements personnels. Ces personnes peuvent être à la recherche de l'adresse de la personne, de son numéro de téléphone, de sa situation financière ou de son état de santé. Les organisations qui possèdent des banques d'informations importantes sur l'ensemble de la population telles que les institutions gouvernementales et financières, les services médicaux, les universités, la police et les services de transport peuvent constituer des cibles intéressantes. Aux États-Unis et en Grande-Bretagne, plusieurs scandales ont mis à jour l'utilisation du *pretexting*[23], c'est-à-dire prétendre être une autre personne afin de tromper et d'obtenir des informations confidentielles. Cependant, le *pretexting* va bien au-delà de simplement mentir sur son identité, le délinquant doit se créer une nouvelle identité et utiliser cette identité pour manipuler sa victime[24] (Hadnagy, 2010). Il doit créer un scénario inventé et à son avantage afin que la cible collabore et lui donne l'information recherchée.

[23] On pourrait traduire le terme *pretexting* par fausse représentation.
[24] Le *pretexting* est largement utilisé dans la fraude par télémarketing,

Cette pratique illégale[25] semble être largement répandue dans le domaine des enquêtes privées. Gill et Hart (1999, p. 250) affirment que ceux qui utilisent le plus les services d'investigateurs privés en Grande-Bretagne sont les compagnies d'assurances, les enquêtes de sécurité, les enquêtes internes, les compagnies de prêts et les compagnies qui collectent les dettes. Cependant, il est difficile d'en mesurer l'ampleur, car il n'y a pas de préjudice économique immédiatement observable et donc peut d'incident sont rapportés à la police.

3.3.3. Les particularités de la communication téléphonique

Considérant que les tentatives d'obtention de renseignements se déroulent au téléphone, il nous semble approprié de soulever certaines particularités de la communication téléphonique. Tout d'abord, bien qu'il y ait une interaction directe entre le présumé fraudeur et l'agent des centres d'appel, il n'y a aucun contact physique entre les deux protagonistes. Dans ce contexte, l'attaquant se sent beaucoup plus en sécurité derrière le téléphone, car tous les signes provenant du langage non verbal tel que l'expression faciale, le mouvement des yeux, la posture du corps, la teinte de la peau, les microdémangeaisons, qui constituent des signes importants dans la création d'une relation avec un inconnu, sont impossibles à identifier au téléphone (Frangopoulos, 2007, p. 71). Ainsi, l'agent ne peut pas utiliser les signes non verbaux pour détecter le mensonge.

Ensuite, la communication téléphonique procure une forme d'anonymat au fraudeur. Celle-ci peut être considérée comme un avantage dans la mesure où il est bien plus facile pour un individu de mentir et de prétendre être quelqu'un d'autre lorsqu'il ne voit pas la personne. De plus, l'anonymat protège le fraudeur contre d'éventuelles poursuites judiciaires, car il est difficile de l'identifier. En plus, différents moyens légaux et illégaux sont disponibles afin de bloquer les traces téléphoniques. Des technologies telles que le *Voice over IP* peuvent être utilisées afin de déguiser la provenance de l'appel. Cet outil, disponible sur les téléphones intelligents, est de plus en plus utilisé et il est très difficile pour les gens de s'apercevoir qu'ils ne parlent pas à la bonne personne. Le téléphone permet également au présumé fraudeur de communiquer avec plusieurs agents et cela en un court laps de temps. Dans le contexte des centres d'appel, cet élément procure un avantage majeur au fraudeur car ce dernier peut tenter d'obtenir des informations sur la même cible autant de fois qu'il le veut. Il peut répéter son stratagème plusieurs fois par jour,

[25] Aux États-Unis, le Gramm-Leach-Bliley Act interdit l'utilisation du pretexting.

car il y a peu de chance que le même agent réponde à l'appel. En répétant son stratagème, il peut aussi tenter de parler avec un agent moins expérimenté ou plus épuisé.

Cependant, l'absence de contact physique oblige le présumé fraudeur à utiliser différentes stratégies pour persuader l'agent que sa demande est légitime. La communication orale étant le principal outil de persuasion, le fraudeur doit bien choisir ses mots et doit utiliser le ton de voix appropriée en fonction des scénarios qu'il crée. Son langage et son attitude verbale doivent être cohérents avec la raison de son appel sinon l'agent refusera l'accès au dossier. Car, pour l'agent, il est aussi plus facile de refuser l'accès à une personne au téléphone qu'en personne.

3.3.4. L'ingénierie sociale

La recension de la littérature sur le vol de renseignements personnels nous a permis de constater qu'autant la menace à la sécurité de l'information que les mesures de protection ne reposent pas dans la sphère technologique. L'une des principales techniques utilisées afin d'obtenir illégalement des renseignements personnels est l'ingénierie sociale. Impliquant différents stratagèmes, l'ingénierie sociale consiste à manipuler les personnes ayant légitimement accès à l'information en utilisant la tromperie et le mensonge (Mitnick & Simon, 2003, p. 41). L'ingénierie sociale fait l'objet de multiples définitions plus ou moins scientifiques. Nous utiliserons celle du *Cyberworld Awareness and Security Enhancement Structure*, une initiative européenne de lutte contre la cybercriminalité, soutenue par l'État du Luxembourg, car elle est particulièrement complète et précise. Selon ces derniers, l'ingénierie sociale est :

> Une technique de manipulation par tromperie qui vise à obtenir l'accès à des informations confidentielles ou à des ressources à accès restreint par la manipulation de personnes en ayant directement ou indirectement l'accès.

L'ingénierie sociale existait bien avant l'avènement de l'informatique, mais il est difficile d'avancer qu'elle est plus utilisée aujourd'hui qu'il y a vingt ans. Cependant, à l'ère de l'information, les systèmes de la sécurité s'organisent et dépendent énormément des technologies au point de mettre l'être humain à un second niveau. Mais tout système de sécurité a un point en commun, il dépend à un moment ou un autre de l'être humain. L'ingénierie sociale attaque précisément ce point vulnérable qu'est l'être humain.

Bien qu'il soit difficile d'évaluer la prévalence de l'ingénierie sociale comme menace à la sécurité de l'information, plusieurs exemples populaires illustrent bien la crédibilité de celle-ci. À ce titre, Kevin Mitnick est l'un des pirates informatiques les plus célèbres, car il a été le premier à être inscrit sur la liste des dix personnes les plus recherchées par le FBI à la fin des années 1980. Il a piraté les bases de données de clients de Pacific Bell, de Fujitsu, Motorola, Nokia, Sun Microsystems, en plus d'accéder illégalement à un ordinateur du Pentagone. Mitnick, maintenant conseiller en sécurité de l'information, utilisait principalement l'ingénierie sociale, notamment par téléphone ou en personne, afin d'obtenir l'accès nécessaire au système. Ainsi, il a démontré qu'il est beaucoup plus simple de manipuler les gens ayant légitimement accès à l'information plutôt que pirater les barrières de sécurité informatique. Ses livres[26], *The Art of Deception: Controlling the Human Element of Security* (2003) et *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers* (2009), illustrent bien l'efficacité de l'ingénierie sociale ainsi que le potentiel qu'elle représente. Cependant, il importe ici de faire la différence entre les attaques qui sont concrètement réalisées et celles qui sont imaginées. Cette distinction nous permettra de nous éloigner des récits qui tiennent davantage de l'anecdote que de la réalité, car nous désirons nous concentrer sur les pratiques qui sont applicables aux délinquants à grande échelle et non pas celles réservées à des pirates très doués qui forment en quelque sorte des exceptions. Dans les prochaines pages, nous présenterons cinq techniques d'influence largement reconnues et documentées.

3.3.4.1. Sympathie et similarité

L'une des techniques les plus efficaces pour influencer une personne est simplement d'être aimable (Cialdini, 1987, p. 159; Nohlberg, 2009b, p. 17). La gentillesse est une attitude efficace pour manipuler les gens, car l'humain est fondamentalement un être social qui aime aider les autres. En adoptant une attitude sympathique et agréable, le fraudeur tentera d'établir une relation de confiance avec l'agent pour que celui-ci réponde positivement à ses demandes (Mann, 2008, p. 87). Selon Workman (2008a), qui étudia à l'aide qu'un questionnaire le comportement de 588 employés d'une compagnie internationale, la confiance est le principal facteur de succès de l'ingénierie sociale. Entre deux inconnus, la confiance peut s'établir de différentes manières soit par l'apparence physique, le lien de similarité entre les personnes ou par l'autorité. Ainsi, les gens

[26] Les deux ouvrages de Mitnick n'ont absolument rien de scientifique, mais ils constituent des mémoires intéressants qui permettent de comprendre cet univers.

qui ont tendance à faire confiance rapidement aux autres sont significativement plus susceptibles d'être victimes de l'ingénierie sociale que ceux qui font moins confiance (Workman, 2008a).

Le principe de la similarité veut que les gens aient tendance à répondre positivement aux personnes avec lesquelles elles partagent un certain nombre de points en commun comme des intérêts, des passe-temps ou un lieu géographique. Cette tendance naturelle à aimer les gens qui leur ressemblent peut être un outil de manipulation efficace (Cialdini, 1987, p. 165). Le fraudeur peut demander à l'agent d'où il vient en raison de son accent, pour ensuite dire que sa femme vient du même endroit. Il peut également demander à l'agent s'il a des enfants de jeunes âges comme lui. Partageant des points en commun, l'agent sera plus enclin à répondre positivement à ses demandes. À l'inverse, le fraudeur peut aussi créer un ennemi commun, par exemple le patron, afin d'établir un contact (Nohlberg, 2009b).

Un autre phénomène intéressant est l'apparence physique d'une personne. Lorsque l'on voit une personne qui a une apparence attirante, on a tendance à croire que tous ses traits de sa personnalité sont égaux à son apparence (Cialdini, 1987). Ce phénomène est appelé l'effet « halo ». Dans les faits, on a tendance à croire qu'une personne qui a une belle apparence est plus honnête, plus intelligente, plus forte, plus aimable que la normale. Bref, quelqu'un qui a une belle apparence peut facilement manipuler plus les gens. Au téléphone, cet effet peut être créé par les mots utilisés par le fraudeur, par la confiance qu'il dégage ou par le poste qu'il prétend occuper.

Afin d'influencer un peu plus une personne à coopérer, Cialdini (1987, p. 14) avance qu'il faut simplement ajouter le mot « parce que » afin de créer l'illusion que la demande est justifiée. En effet, il relate une expérience élaborée par Ellen Langer (1978) de l'Université de Harvard qui consistait à demander à 120 personnes qui attendaient dans une ligne pour effectuer des photocopies s'il était possible de passer avant eux. Lors de la première tentative, la personne se contentait de dire : Pardon, je n'ai que cinq pages. Est-ce que je peux prendre la machine? Dans ce cas, soixante pour cent (60%) des personnes ont accepté. Lors de la seconde tentative, elle formulait sa requête ainsi : Pardon, je n'ai que cinq pages. Est-ce que je peux prendre la machine, parce que je suis pressé? Quatre-vingt-quatorze pour cent (94%) l'ont laissé passer. Finalement, lors de la troisième tentative, elle dit : Pardon, je n'ai que cinq pages. Est-ce que je peux prendre la machine parce qu'il faut que je fasse des photocopies? Dans ce cas, quatre-vingt-treize pour cent (93%) des personnes ont accepté alors qu'aucune information supplémentaire ne pouvait

justifier qu'ils accepteraient. Selon Cialdini, l'utilisation du mot «parce que» enclenche une réponse positive automatiquement et cela peu importe la justification donnée.

Dans le même ordre d'idées, les résultats du psychologue américain Paul Slovic, l'un des plus importants chercheurs travaillant sur le processus décisionnel et le jugement, montre que dans des situations où un choix est particulièrement difficile à faire en raison d'un haut degré d'incertitude quant aux conséquences d'une action, l'être humain ne prend pas la décision en fonction du choix le plus rationnel, mais en fonction de celle qui est la plus facile à justifier (Slovic, 1975). Dans cette optique, la quantité d'information plutôt que la qualité de celle-ci influencera une personne à coopérer.

3.3.4.2. Réciprocité

La réciprocité est une norme sociale profondément ancrée dans l'humain. Ce principe, aussi connu sous le nom d'engagement, veut que si quelqu'un nous rend un service, on se doit de lui donner quelque chose en retour même si l'on a rien demandé initialement. Des sociologues ont étudié ce phénomène et selon eux, il s'agit d'une règle universelle à l'essence même de la société humaine, car elle permet à l'humain de s'adapter en partageant leur compétence (Cialdini, 1987, p. 26). Aujourd'hui, ce principe informel de réciprocité est particulièrement puissant alors que ceux qui ne le respectent pas sont considérés comme ingrats et profiteurs. Cependant, certains individus peuvent profiter de ce sentiment d'obligation.

Ce phénomène, connu sous le nom de pied dans la porte, a été étudié pour la première fois par les psychologues Jonathan Freedman et Scott Fraser (1966). Ces derniers voulaient savoir si le simple fait de réaliser un acte des plus anodins (donner l'heure, des directions ou signer une pétition) ne nous prédisposait pas à accepter, plus favorablement, une requête ultérieure bien plus coûteuse en temps et en argent (Guéguen, 2002, p. 86). Bien que l'acceptation de la requête initiale ne mène pas systématiquement à l'acceptation de la demande finale, elle augmente considérablement les chances de succès. Un fraudeur peut utiliser cette technique en commençant par aider la victime concernant un petit problème, sans que celle-ci lui ait demandé de l'aide, ou en donnant un privilège qu'elle n'a pas demandé (Nohlberg, 2009a). La victime se sentira alors plus encline à répondre positivement à une demande ultérieure du fraudeur afin de lui rendre sa faveur.

Dans le même ordre d'idées, la technique intitulée la porte dans le nez, consiste à commencer par une demande élevée pour ensuite atteindre un niveau de base (Guéguen, 2002, p. 119). Cette technique est très utilisée en vente et se base sur le principe de la concession réciproque (Cialdini, 1993). En fait, l'importance n'est pas tant le prix que la concession qui est faite. Cette norme de réciprocité implique qu'une personne fera des concessions à celui qui lui en a fait. Un fraudeur peut faire une demande irraisonnable sachant très bien que l'agent ne pourra lui donner. Par la suite, il dira qu'il veut seulement savoir une petite chose insignifiante et l'agent acceptera. Cependant, l'agent n'aurait pas jugé raisonnable de donner cette information si la demande irraisonnable n'avait pas été faite préalablement.

3.3.4.3. Preuve sociale

Le principe de la preuve sociale signifie que dans l'incertitude, un individu reproduit le comportement du plus grand nombre, s'appuyant sur l'hypothèse que si beaucoup de gens le font, alors c'est bien. Nous jugeons qu'un comportement est plus approprié à une circonstance particulière si nous voyons d'autres personnes l'adopter (Cialdini, 1987, p. 113). Dans ce principe, plus de gens croient qu'une idée est correcte, plus l'idée sera correcte. Ce phénomène, observable dans une multitude de situations, peut avoir un impact important en matière de sécurité, car les membres d'une entreprise vont adapter leur comportement à l'attitude générale des employés par rapport à la sécurité. Si l'attitude des employés est que la sécurité peut être négligée alors tout le monde agira de cette manière. Ce type de phénomène engendre une forme de conformité où ceux qui ne s'y rattachent pas sont identifiés comme ne faisant pas partie du groupe. Ainsi, ceux qui se conforment aux règles que le groupe ne respecte pas sont considérés comme déviants. Concrètement, un fraudeur va utiliser cette technique de persuasion en disant à l'agent que tout le monde le fait donc, pourquoi ne pas le faire.

3.3.4.4. Autorité

Le quatrième principe est celui de l'autorité. D'un point de vue de l'organisation sociale, l'autorité est largement acceptée, car il y a de nombreux avantages à la respecter. Elle permet de mettre en place des structures complexes de production, de commerce, de défense, d'expansion et d'ordre social qui seraient sans elle impossibles (Cialdini, 1987, p. 205). Une société où il n'y a aucune autorité est anarchique. Individuellement, nous apprenons très jeune à répondre positivement à l'autorité, qu'il s'agisse du milieu familial, scolaire ou professionnel, car il y a des

bénéfices à la respecter. L'étude de Stanley Milgram (1974), *Obedience to Authority*, concernant la soumission à l'autorité, est la plus célèbre. En effet, les résultats de l'étude de Milgram, qui consistait à ce qu'un participant donne, en présence d'un professeur qui faisait figure d'autorité, une décharge électrique à une autre personne si celle-ci commettait une erreur de mémorisation, sont très intéressants. Avant l'expérience, les participants, des gens ordinaires, avaient eu comme consigne que l'usage des chocs constituait la partie essentielle de l'expérience. Soixante-cinq pour cent (65%) des participants ont sans contrainte coercitive, infligée trente décharges de plus en plus élevées jusqu'à atteindre la décharge maximale de 450 volts, à l'autre personne et cela, en entendant ses cris de douleur et en sachant que la décharge occasionnait de grandes souffrances et des dommages physiques importants. Évidemment, la personne qui recevait les décharges factices était un membre de l'équipe de Milgram. Cette expérience fut répétée à plusieurs endroits dans le monde et les résultats sont toujours aussi convaincants.

L'autorité est une position de pouvoir qui permet de donner des récompenses, mais également des sanctions à une autre personne. Ainsi, l'autorité peut être utilisée pour créer un sentiment de peur où les personnes obéissent afin d'éviter des conséquences négatives (Cialdini, 1987). Selon Workman (2008a, p. 467), les gens, qui ont peur de subir des conséquences négatives, vont obéir automatiquement aux demandes d'une personne en autorité et elles sont plus susceptibles d'être victimes d'ingénierie sociale.

Tout dépendant du contexte, différents facteurs influencent ce qui est perçu comme une figure d'autorité. Il peut s'agir d'uniformes (police, docteur, soldat, électricien, entretien ménager, complet très luxueux), de titres professionnels (docteur, maître, président, ingénieur), d'accessoires (voiture de luxe, cellulaire, montre) ou l'utilisation d'un jargon très précis à un domaine (Cialdini, 1993). L'utilisation de ces symboles d'autorité influence fortement la prise de décision même qu'elle enclenche la plupart du temps des automatismes. Lorsqu'une personne se présente comme policier, nous modifions automatiquement notre comportement et cela, sans remettre en question cette autorité. Ainsi, l'appel à l'autorité est l'un des principes les plus utilisés en ingénierie sociale. Afin de projeter une image d'autorité lors de communication téléphonique, les fraudeurs utilisent souvent des titres professionnels et un langage spécifique.

3.3.4.5. Rareté

Le dernier principe est celui de la rareté. Pour la majorité des gens, ce qui est peu disponible a plus de valeur que ce que l'on trouve en abondance. Ainsi, la rareté fonctionne parce que l'on croit toujours que les bonnes choses sont rares. En vente, des services ou des produits sont souvent offerts pour un temps très limité et la décision doit être prise maintenant, car des facteurs externes font qu'ils ne seront plus disponibles plus tard. Dans ce contexte, le traitement de l'information et la qualité de la décision sont généralement inférieurs à une décision prise dans un contexte normal.

En matière de fraude au téléphone, ce principe est utilisé, car le facteur temps pousse souvent les gens à prendre des décisions moins réfléchies. L'urgence est une composante fréquemment utilisée dans les messages frauduleux (Langenderfer & Shimp, 2001). Par exemple, le fraudeur va demander à la cible de prendre une décision rapidement, car il doit partir. Le fraudeur peut également contacter la cible à des heures stratégiques, soit en fin de journée à quelques minutes de la fermeture afin d'utiliser le temps en sa faveur. Pour les centres d'appel, cet élément est d'autant plus pertinent que l'agent doit respecter un temps d'appel. Il doit répondre à la demande du client dans un minimum de temps. Ainsi, l'agent sera plus enclin à donner des informations plus rapidement s'il sait qu'il a dépassé son temps moyen de traitement et que ses statistiques personnelles seront affectées.

4. LA PROBLÉMATIQUE

Les statistiques officielles sur la perte de renseignements personnels indiquent qu'il s'agit d'un phénomène présent et en expansion. Lors des huit dernières années, selon le *Data base loss*, 3 023 cas de pertes de renseignements personnels impliquant 616 448 217 dossiers ont été signalés aux États-Unis[27]. D'un point de vue social, ces pertes, bien qu'elles n'impliquent pas systématiquement une utilisation criminelle, sont préoccupantes, car le vol d'information n'est habituellement pas une fin en soi, mais plutôt un outil qui facilite ou permet de commettre d'autres crimes tels que la fraude. La perte de renseignements personnels peut être en quelque sorte considérée comme la source de multiples problèmes criminels.

[27] Cette tendance est également présente dans les statistiques compilées par l'*Identity Theft Resource Center*, une organisation sans but lucratif qui collecte, elle aussi, les informations disponibles sur les pertes de renseignements personnels aux États-Unis.

Mais au-delà des pertes officiellement signalées, se trouve un important chiffre noir qui correspondrait aux accès non autorisés à des renseignements personnels qui ne sont pas détectés. Au Canada, le phénomène est d'autant plus difficile à saisir, car il n'existe aucune obligation légale de signaler la perte de renseignements personnels et par conséquent, aucune statistique officielle n'est disponible afin d'évaluer l'ampleur du problème. Cependant, il n'y a aucune raison de croire que la situation est meilleure au Canada qu'aux États-Unis. De plus, bien que le phénomène suscite un intérêt relatif au niveau politique, plusieurs cas de pertes de renseignements personnels mobilisent de plus en plus l'attention médiatique. Si la tendance se maintient, il est fort probable que la protection des renseignements personnels occupera une place de plus en plus importante dans les débats publics.

Le vol et la perte de renseignements personnels sont des problèmes sérieux, car ils peuvent avoir d'importantes conséquences pour le client victime, autant financières que psychologiques, mais également pour l'institution qui a la responsabilité légale, selon la LPRPDÉ, de les protéger. Occupant un rôle fondamental dans les sociétés modernes, la protection de la vie privée est un enjeu qui fait partie intégrante de la collecte de renseignements personnels. Légalement, une organisation ne peut pas communiquer des renseignements personnels à un tiers sans le consentement de la personne en question. Or, lorsqu'un présumé fraudeur prétend être un client de l'organisation et qu'il réussit le protocole d'identification, des renseignements sur le client sont communiqués à un tiers sans son autorisation. Outre les possibles conséquences légales, ces incidents peuvent entacher la réputation, engendrer d'importantes pertes financières et miner la confiance du public envers l'organisation.

La littérature sur la psychologie nous a permis d'identifier plusieurs techniques de manipulation possiblement utilisées par les fraudeurs. Cependant, on retrouve relativement peu de connaissances empiriques sur les techniques utilisées par les fraudeurs afin d'obtenir de l'information confidentielle. Les raisons de ce vide sont multiples. Tout d'abord, très peu d'organisations mettent en place des systèmes de sécurité comprenant la collecte d'information sur des tentatives non autorisées d'obtention de renseignements personnels. Bien que la majorité des organisations ont des mesures de sécurité afin d'authentifier l'identité du client, très peu ont en place un système pour collecter de l'information sur les cas de tentatives de fraude lorsqu'elles sont détectées. Lorsque c'est le cas, il s'agit d'une source d'information confidentielle, qu'elles ne souhaitent pas partager par crainte d'effrayer le public.

Ensuite, il arrive que des personnes utilisant l'ingénierie sociale divulguent volontairement les techniques utilisées pour obtenir de l'information confidentielle. Cependant, il s'agit souvent des spécialistes qui ont élaboré des modèles d'attaque complexes ce qui fait en sorte que les événements rapportés diffèrent grandement des attaques réelles dans la mesure où elle demande énormément de préparation et de talent. On s'approche davantage des cas probables ou imaginés que des cas de fraude réalisés concrètement.

Par la suite, la troisième source d'information généralement disponible sur les cas de vol d'information provient des victimes. Cependant, ces données souffrent habituellement d'un manque des détails, car il s'écoule une période de temps entre le moment où la victime se fait manipuler et le moment où elle rapporte l'événement aux autorités. Dans ce contexte, disposant de très peu d'information, les autorités ne peuvent pas mener des enquêtes et porter des accusations. De plus, à moins d'avoir subi directement d'importantes pertes financières, il est plutôt rare que les victimes portent plainte aux autorités. Bref, les preuves empiriques sur les techniques utilisées pour tromper les gens afin d'obtenir des renseignements personnels ont plusieurs lacunes.

Notre projet de recherche permet de remédier à plusieurs des limites mentionnées plus tôt en utilisant une méthodologie unique. En effet, cette recherche exploite deux sources d'information privilégiée, soit les connaissances des agents des centres d'appel devant gérer les tentatives et les fiches de signalement qui constituent la mémoire de l'organisation. Basées uniquement sur des cas réels de tentatives d'obtention non autorisées de renseignements personnels, ces données sont un support empirique majeur dans l'identification des stratégies utilisées par les délinquants à grande échelle. Ces informations sont d'autant plus intéressantes qu'elles sont le fruit d'une interaction entre le délinquant, qui parvient parfois à obtenir de l'information confidentielle, mais qui échoue également dans ses tentatives, et l'agent des centres d'appel qui réussit à détecter les présumés fraudeurs.

Cependant, cette interaction prend place dans un contexte organisationnel particulier. Dans notre cas, diminuer l'influence de l'environnement dans l'explication du phénomène serait une grave erreur. En fait, l'originalité du projet est de ne pas se contenter de décrire simplement les techniques utilisées par les présumés fraudeurs, mais bien d'intégrer des composantes de la menace et de l'organisation victime, chargée de protéger l'information. Ainsi, nous croyons que l'explication du phénomène de vol de renseignements personnels passe par la mise en relation des particularités de l'ingénierie sociale et des centres d'appel. Notre démarche se démarque par l'intégration de ces deux composantes dans l'analyse du phénomène. Pour y arriver, nous avons exploité toutes les sources d'information possibles en concentrant nos énergies sur le travail des agents qui sont responsables de détecter et de signaler les tentatives non autorisées d'obtention de renseignements personnels.

Cette recherche permettra de définir les caractéristiques d'une menace réelle pour toute organisation détenant des renseignements personnels, mais dont peu semblent être conscientes de sa forme, de son ampleur et de sa portée. Les connaissances développées pourraient être importantes pour la gestion des risques lors de communication de renseignements personnels et pourraient influencer les organisations à actualiser leurs politiques et procédures. De plus, compte tenu du fait que les centres d'appel sont un système de gestion répandu, les connaissances développées lors de cette recherche seront transférables à diverses instances publiques provinciales, fédérales et organisations privées.

Enfin, contrairement à la majorité de la littérature scientifique qui considère la protection de l'information comme une responsabilité informatique, ce projet accorde une place prépondérante à l'élément humain et contribuera à développer des connaissances axées sur l'importance de l'intégration du facteur humain dans la protection de l'information.

De façon générale, notre problématique de recherche tente de déterminer les caractéristiques des stratégies utilisées par les présumés fraudeurs pour obtenir des renseignements personnels. À l'aide de la méthodologie appropriée, nous nous proposons d'atteindre les objectifs suivants :

- Présenter la fréquence et l'ampleur des tentatives non autorisées d'obtention de renseignements personnels pour l'organisation.
- Comprendre la manière dont les tentatives non autorisées d'obtention de renseignements personnels est perçue et gérée sur le terrain par les agents du centre d'appel.
- Décrire les éléments qui semblent être exploités par les présumés fraudeurs lors des tentatives non autorisées d'obtention de renseignements personnels.
- Décrire la position organisationnelle des agents et son impact sur la protection des renseignements personnels.

CHAPITRE II :

LA DÉMARCHE ET

LES DONNÉES EMPIRIQUES UTILISÉES

Cette section présente la méthodologie utilisée dans le cadre de ce mémoire. Tout d'abord, nous présenterons les raisons qui ont motivé l'utilisation d'une démarche qualitative. Ensuite, nous exposerons les stratégies d'échantillonnage et le profil des agents rencontrés. Par la suite, nous décrirons le déroulement de la cueillette des données. Enfin, nous présenterons les stratégies d'analyse préconisée ainsi que quelques limites de la recherche.

1. LE CHOIX DE LA MÉTHODE DE RECHERCHE

Afin d'atteindre notre principal objectif de recherche, qui est de décrire les tentatives non autorisées d'obtention de renseignements personnels, nous avons privilégié une démarche qualitative. Certes, nous aurions pu nous contenter d'analyser la base de données des signalements compilés par l'organisme public. Il ne fait aucun doute que celle-ci est pertinente dans la description du phénomène, car elle contient une section où les agents décrivent la tentative d'obtention de renseignements personnels et elle procure de nombreuses données sur les stratagèmes utilisés par les fraudeurs. Cependant, prises hors contexte, ces fiches sont difficilement interprétables. Ainsi, il nous semblait indispensable de réaliser des entretiens avec les acteurs clés de ce phénomène afin de bien saisir la complexité des cas de fraude.

Il nous semblait donc essentiel de recueillir les connaissances développées par les agents et leur point de vue sur cette problématique afin de bien analyser le phénomène (Mason, 2002, p. 63). Qui plus est, les tentatives non autorisées d'obtention de renseignements personnels sont le résultat d'une interaction entre l'agent et le présumé fraudeur et la démarche qualitative était la plus adaptée afin de recueillir les informations sur cette dynamique. Il ne fait aucun doute que l'idéal aurait été d'obtenir le point de vue des deux protagonistes, ou du moins, d'avoir accès aux enregistrements audio des conversations. Or, très peu de conversations sont enregistrées dans l'organisation et elles sont seulement utilisées pour s'assurer de la qualité du service. Ainsi, nous sommes conscients que nous analysons seulement cinquante pour cent (50%) de l'interaction et que le discours de l'agent, que ce soit oral ou écrit, est en fait une reproduction des événements selon son point de vue. Cependant, il s'agit d'une contrainte inhérente à notre recherche.

Ensuite, notre recension des écrits sur la sociologie des centres d'appel nous avait permis de saisir l'impact de cet environnement sur le travail de ses employés. Il nous était donc

indispensable de questionner les agents à ce sujet et seuls des entretiens nous permettaient de comprendre la complexité de l'environnement et de son impact sur le travail des agents. Donc, notre source primaire d'information est les entretiens avec des agents des centres d'appel. Par la suite, nous avons complété notre terrain par une analyse documentaire des fiches de signalement de tentatives d'obtention de renseignements personnels. Ces deux sources empiriques sont très complémentaires et elles nous permettent d'effectuer une analyse en profondeur du phénomène. Le croisement des données quantitatives et qualitatives nous permet d'assurer une objectivité supplémentaire dans notre présentation du phénomène.

1.1. Entretien semi-dirigé

En tant qu'acteur de première ligne, il nous semblait primordial d'effectuer des entretiens avec les agents. Devant gérer les appels suspects, les agents dans les centres d'appel sont sans aucun doute les mieux placés pour décrire ce type de phénomène. En fait, ils sont les informateurs clés et une exploration en profondeur de leur perception du phénomène et de leur travail est indispensable à une juste compréhension du phénomène (Jaccoud & Mayer, 1997).

Nous avons donc opté pour la réalisation d'entretiens semi-directifs, car ceux-ci permettent de bien comprendre les expériences, les pratiques et le point de vue des agents. Tout en laissant une certaine liberté, cette méthode de collecte de données assure un questionnement continu et une fluidité d'interaction entre le chercheur et l'agent. Selon Quivy et Van Campenhoudt (1995), ce type d'entretien permet de nous recentrer sur les objectifs, chaque fois que l'entretien s'en écarte et permet également de poser les questions que l'interviewé n'aborde pas de sa propre initiative. Enfin, cette approche nous a permis de recueillir un plus grand nombre d'informations, dont certaines qui auraient pu nous échapper avec d'autres modes de collecte des données.

Considérant que les tentatives d'accès sont un élément dont les agents n'ont pas l'habitude de discuter avec des personnes de l'extérieur, il nous semblait important de laisser l'agent évoquer les thèmes qu'il jugeait pertinent afin que nous puissions saisir leur compréhension et leur perception du phénomène. Ainsi, cette démarche nous a permis d'identifier la singularité dans les discours des agents. Cependant, les entretiens semi-dirigés nous ont permis d'aborder les thèmes

moins développés par l'agent, mais qui nous semblait tout de même pertinents dans le cadre de cette recherche.

1.2. Rencontre en groupe

Afin de compléter notre échantillon, nous avons également réalisé des entretiens avec deux groupes d'agents. Cette méthodologie, populaire en raison de sa flexibilité, consiste à réunir un petit groupe de personnes afin que celles-ci discutent informellement d'un sujet particulier (Wilkinson, 2004, p. 78). Cette stratégie connexe aux entretiens semi-dirigés nous a permis de rencontrer onze (11) agents supplémentaires et elle a été mise en place en raison du nombre limité d'agents que nous pouvions rencontrer individuellement car la rencontre avec des agents entrait en conflit avec de nouveaux objectifs organisationnels. En effet, la direction du centre d'appel avait revu plusieurs processus au sein de l'organisation afin d'augmenter la productivité du centre d'appel. Les objectifs de rendement des agents avaient notamment été revus à la hausse. Il était donc contradictoire pour la direction de demander aux agents de participer aux entrevues et de relayer la productivité à un second niveau. Ainsi, nous avons dû modifier notre stratégie initiale qui était de rencontrer vingt (20) agents individuellement. Cependant, cette méthode s'est avérée intéressante dans la mesure où la dynamique des rencontres a favorisé le partage de cas vécus et l'émergence de nouveaux points de vue. Comme le souligne Morgan (1997, p. 15), les échanges que les participants font sur leurs expériences et leurs opinions sont une source d'information précieuse et unique, que nous avons eu la chance d'exploiter.

De plus, comparativement aux entretiens individuels, les groupes de travail permettent d'obtenir une quantité importante d'information en un court laps de temps. Évidemment, les informations obtenues sont moins détaillées, car les participants n'ont pas le temps d'aller en profondeur. Cette démarche apportait un complément intéressant à notre recherche, car nous avions déjà eu l'occasion d'aller en profondeur lors des huit entretiens semi-dirigés que nous avions réalisés auparavant.

1.3. Base de données

Comme troisième source d'information, nous avons obtenu l'autorisation de l'organisation afin d'utiliser la base de données contenant tous les signalements enregistrés par les agents. Alors que les entretiens avec les agents nous ont permis de bien cerner la gestion des appels suspects, l'analyse de la base de données des signalements de tentatives non autorisées d'obtention de renseignements personnels nous a permis de recueillir de nombreuses informations sur les stratagèmes utilisés par les présumés fraudeurs. Car, si les rencontres avec les employés nous permettaient de mieux saisir la perception des acteurs et le contexte organisationnel, ceux-ci se souvenaient de peu de détails sur les cas de fraude. Ainsi, l'utilisation des fiches de signalement a comblé efficacement cette lacune. Au moment de l'analyse de la base de données, 1 136 signalements avaient été enregistrés.

Collectée depuis quatre ans, la base de données contient des informations qualitatives sur les cas de fraude. En effet, à la suite de chaque tentative détectée, l'agent doit remplir une section décrivant le déroulement de l'appel. Étant complétée immédiatement après l'événement, cette section contient de nombreuses informations utiles sur les tactiques utilisées par les présumés fraudeurs et sur l'interaction avec l'agent. Cependant, pour l'agent, cette section est la plus longue à remplir et elle est parfois complétée rapidement. En d'autres mots, les fiches ne sont pas complétées à des fins scientifiques et certaines ne sont tout simplement pas adaptées à une analyse. Ainsi, nous avons effectué une première sélection en prenant soin de retenir seulement les signalements dont la qualité de la description de l'événement permettait une analyse. Par la suite, nous avons effectué une deuxième sélection en résonnance avec les propos des agents, des discussions avec la responsable des signalements et la littérature sur la fraude. Nous avons donc retenu cent quatre-vingt-douze (192) tentatives non autorisées.

La base de données sur les signalements contient également des informations quantitatives sur la date et l'heure de tentatives, les informations que possédait le présumé fraudeur et celles recherchées et son sexe. Toutefois, cette base n'est pas faite pour des analyses statistiques complexes. Nous nous sommes donc contentés d'analyses descriptives. Évidemment, nous sommes conscients que les statistiques donnent davantage un aperçu du travail des agents à signaler que du taux réel de tentatives non autorisées d'obtention. Ainsi, une augmentation du

nombre de signalements ne signifie pas nécessairement davantage de tentatives non autorisées, mais peut-être une plus grande vigilance de la part des agents. Cependant, considérant que nos objectifs de recherche ne visent pas à évaluer avec précision l'ampleur du problème, elle représente une source d'information pertinente à exploiter et à présenter.

2. LA STRATÉGIE D'ÉCHANTILLONNAGE

L'organisation où la recherche a eu lieu possède cinq centres d'appel au Québec qui se partagent quatre secteurs de services distincts. Lors des mois de février et de mars 2010, nous avons réalisé une journée d'entrevues exploratoires dans chacun des services afin d'effectuer la sélection de l'environnement le plus approprié pour la recherche. Deux éléments ont motivé le choix d'un centre d'appel en particulier. Tout d'abord, nous avons choisi le centre d'appel où les employés avaient le plus de responsabilités. Ceux-ci accédaient très régulièrement au dossier des clients et ils pouvaient y effectuer des modifications (changement d'adresse, numéro de téléphone, état du dossier). En plus, il s'agissait de l'un des centres d'appel les plus occupés. Ensuite, considérant qu'il n'y avait pas de centres d'appel dans la grande région de Montréal, nous avons tenu compte de la proximité géographique afin de faciliter les déplacements. Les tâches des agents du centre d'appel sont de transmettre des renseignements généraux sur les services offerts par l'organisation, de mettre à jour les dossiers du client, de transmettre l'information de son dossier au client et d'assurer le suivi des dossiers. L'organisme public en question offre un service à l'ensemble de la population québécoise et dans certains cas le citoyen est obligé (légalement) de prendre des arrangements avec l'organisme.

Sur le plan théorique, considérant que notre recherche porte sur une institution bien circonscrite, un organisme public, et plus précisément, sur les agents aux services à la clientèle, notre échantillon est défini par le milieu de travail (Pires, 1997, p. 125). À partir de cette population, qui compte environ quatre-vingts (80) employés, nous avons sélectionné un échantillon représentatif de l'environnement de travail tout en prenant soin d'obtenir une diversité de point de vue. Ainsi, notre premier critère a été d'avoir autant d'agents qui avaient déjà effectué un signalement que d'agents qui n'avaient jamais signalé. Dans notre échantillon, 58% avaient déjà effectué un signalement. Cependant, le fait de n'avoir jamais signalé n'impliquait pas que l'agent n'avait jamais fait face à une tentative non autorisée d'obtention de renseignements personnels.

Ainsi, quatre-vingt-quatre pourcent (84%) des agents rencontrés ont dit avoir déjà eu l'impression, même si le protocole d'identification avait été réussi, qu'il avait affaire à un présumé fraudeur. Nous avons choisi ce critère afin d'obtenir une diversité de point de vue sur le phénomène, car si nous avions seulement rencontré des agents qui signalent fréquemment, nous aurions eu une fausse représentation du travail et de la perception des agents en général. Ensuite, nous souhaitions rencontrer des agents comptant un nombre d'années d'expérience variées, car cela influence la manière dont les cas de fraude sont gérés. Enfin, nous souhaitions rencontrer un nombre d'hommes représentatif du rapport homme / femme dans le centre d'appel.

Notre échantillon a été élaboré en collaboration avec la directrice adjointe du centre d'appel. Tout d'abord, nous lui avons communiqué nos trois critères de sélection. Par la suite, elle a approché les chefs d'équipe, qui supervisent environ douze (12) employés chacun, pour que ceux-ci informent les employés et qu'elle communique le nom des volontaires. Enfin, la directrice nous transmettait la liste des personnes intéressées. Un courriel d'une page expliquant le projet de recherche avait été préalablement envoyé à tous les employés du centre d'appel[28]. Finalement, notre stratégie a permis de rencontrer un total de dix-neuf (19) employés. Au sein de notre échantillon, nous avons rencontré huit (8) agents individuellement et deux groupes comptant au total onze (11) personnes. Tous les agents ont participé volontairement aux rencontres et ils avaient suivi la même formation et ils occupaient les mêmes fonctions.

2.1. Profil des participants

Notre échantillon comprend dix-neuf (19) employés, dont seize (16) femmes et trois (3) hommes. Cette surreprésentation des femmes dans notre échantillon est volontaire car elle reflète la proportion d'hommes et de femmes dans l'environnement de travail. Les agents sont âgés de 23 à 59 ans. La moyenne d'âge étant de 41 ans. Les agents comptent une moyenne de six (6) années d'expérience dans des centres d'appel de l'organisation. Quarante-deux pourcent (42%) d'entre eux possèdent un diplôme universitaire.

[28] Vous trouverez le courriel en Annexe I.

3. LA CUEILLETTE DES DONNÉES

3.1. Contexte des entretiens

La cueillette des données a eu lieu en deux temps. Tout d'abord, nous avons réalisé huit (8) entrevues semi-directives entre les 20 et 28 mai 2010. Par la suite, nous avons rencontré les groupes de travail les 7 et 21 juillet 2010. La durée des entretiens a varié entre 50 et 95 minutes. La moyenne a été d'une heure et les entretiens ont été enregistrés avec l'autorisation de l'employé afin de faciliter l'analyse de l'information.

Les entretiens ont eu lieu au centre d'appel lors des heures régulières de travail soit entre 9 h et 16 h. Nous avons opté pour rencontrer les agents à leur bureau afin qu'il soit le plus possible dans leur environnement quotidien et qu'il produise un discours le plus près possible de la réalité. Selon Poupart (1998, p. 198), si les conditions se rapprochent le plus possible des conditions de la vie quotidienne de l'interviewé, les artifices de la situation d'entretien en seront atténués, celui-ci se sentira plus à l'aise. Quant au groupe de travail, les deux rencontres ont eu lieu dans une salle de conférence dans les bureaux de l'organisation en début de journée.

Dès le début des entretiens, nous prenions quelques instants pour spécifier que nous ne représentions pas l'organisation et que l'objectif de la rencontre n'était pas d'évaluer leur travail. Après avoir discuté du processus qui nous avait amené à rencontrer les agents de ce centre d'appel, nous avons mentionné que l'objectif général du projet était d'utiliser leurs connaissances sur les tentatives d'obtention de renseignements personnels afin de dresser un portrait plus complet et réaliste de la situation à l'organisation. Notre consigne de départ consistait à demander à l'agent quelle était son appréciation de la principale mesure de sécurité qu'il doit appliquer, le protocole d'identification. Ensuite, nous enchainions avec les situations ambigües que pouvait engendrer l'application du protocole, dont les tentatives non autorisées d'accès. Enfin, une fois l'entrevue terminée, nous demandions à l'agent de compléter une fiche signalétique afin de compiler des renseignements d'ordre général sur les répondants[29].

[29] Vous trouverez un exemple de la fiche signalétique en Annexe III. Nous y avons également compilé les résultats des dix-neuf (19) employés rencontrés.

3.2. Thèmes abordés

Grâce aux entretiens exploratoires que nous avions réalisés dans les différents centres d'appel de l'organisation, nous avions élaboré une grille contenant les trois principaux thèmes que nous désirions abordés lors des entretiens semi-directifs[30]. Tout d'abord, nous cherchions de l'information sur la perception qu'ont les agents des situations de tentatives d'obtention de renseignements personnels. Nous désirions savoir ce que les agents considéraient comme une tentative d'obtention non autorisée. Alors que notre thème de départ consistait seulement à connaître la perception des agents du problème d'obtention de renseignements personnels, nous avons senti le besoin, très tôt dans les premiers entretiens, de connaître comment les agents traçaient la ligne entre ce qu'il considérait comme une tentative et ce qu'il considérait comme anodin. Dans ce thème, nous voulions également que les agents nous décrivent des situations vécues, les signes permettant d'identifier les appels suspects, les techniques utilisées par le présumé fraudeur et la manière dont l'agent avait géré la situation. Comme nous l'avions prévu, les agents avaient relativement peu d'information sur la fréquence et la forme des cas de fraude, mais ils sont parvenus à nous décrire la manière dont ils gèrent les situations où ils doivent refuser l'accès au requérant. Ces situations peuvent inclure des cas de tentatives non autorisées tout comme des demandes légitimes. Ils ont également été en mesure de nommer plusieurs signes suspects qui font en sorte qu'ils appliquent plus rigoureusement le protocole ou qu'ils refusent l'accès.

Ensuite, le deuxième grand thème que nous souhaitions développer était le dilemme entre la productivité, le service à la clientèle et l'application du protocole. La littérature scientifique sur la sociologie des centres d'appel nous avait permis de saisir la complexité de cet environnement ainsi que les vulnérabilités qui s'y rattachent. Ces thèmes ont en effet été très riches en information car les agents étaient très interpellés par ce dilemme. En ajoutant l'élément de sécurité dans la dynamique de la productivité et du service à la clientèle, nous croyons être en mesure de diviser ce thème en trois sous-thèmes bien distincts. Or, à la suite d'une première catégorisation, nous avons réalisé qu'ils se chevauchaient trop et qu'il était préférable de les réunir. Ce thème, nous a permis d'identifier des points de vue diversifiés sur l'importance que chaque agent accorde à la productivité, au service à la clientèle et à l'application du protocole. Enfin, le dernier thème consistait à connaître leur appréciation des mesures de sécurité en place et

[30] Vous trouverez en Annexe II, la grille d'entretien utilisée lors des rencontres avec les employés.

les pistes d'amélioration possibles. Nous cherchions des informations sur la formation et la sensibilisation reçues, la fiche de signalement et le processus qui l'entoure.

4. L'ANALYSE DES DONNÉES

Pour des fins d'analyse, nous avons retranscrit toutes les entrevues sous forme de verbatim. Ensuite, nous avons effectué une première lecture verticale de chaque entretien afin de codifier en catégorie les passages pertinents. Pour toutes les étapes d'analyse, nous avons utilisé le logiciel QDA Miner. Cette première codification nous a permis de réduire la quantité de matériel à analyser. Une lecture verticale de chaque entretien permet d'obtenir une compréhension individuelle du phénomène. Par la suite, nous avons procédé à une seconde lecture, cette fois-ci horizontale afin de dégager les rapports entre les thèmes dans une optique plus globale qu'individuelle. Cette stratégie nous a permis d'identifier des similitudes ainsi que des divergences entre les acteurs sur des thèmes spécifiques. Cette lecture transversale nous a également permis de distinguer les stratégies les plus récurrentes et les prétextes fréquemment utilisés par les présumés fraudeurs. Afin de faciliter l'analyse et l'interprétation des données, nous avons utilisé les mêmes catégories pour coder les verbatims et les fiches de signalement.

Cependant, afin d'identifier efficacement les stratégies mises en place par les présumés fraudeurs, nous avons utilisé le concept de *script* développé par Cornish (1994). Ce concept permet d'illustrer graphiquement ou à l'aide de tableaux, les modus operandi du criminel ainsi que les détails du crime. Lors des dernières années, les crimes d'appropriation tels que le vol et la fraude ont été des terrains de recherche particulièrement fructueux pour identifier les *modus operandi* des criminels.

En fait, selon Cornish et Clarke (Cornish & Clarke, 2002, p. 47), tous les crimes peuvent être considérés comme un enchaînement d'action et de décisions interdépendantes dans le but d'atteindre un objectif. Afin de faciliter l'analyse d'un phénomène criminel, il est plus efficace de diviser et d'identifier les étapes qui structurent le crime. Ainsi, selon les étapes, il est possible de choisir parmi plusieurs configurations d'interventions possibles (Cornish & Clarke, 2002, p. 48). De plus, ce type d'analyse permet de stimuler la pensée sur de nouvelles manières de combattre le crime (Cornish & Clarke, 2002, p. 48).

Ce cadre d'analyse nous a permis de mettre à jour les *modus operandi* employés par la majorité des présumés fraudeurs et d'illustrer l'interaction entre le criminel et les agents de l'organisme public. De plus, cette approche nous a permis de soulever les éléments situationnels influençant la séquence d'action afin d'offrir un portrait beaucoup plus réaliste de la complexité de l'événement criminel. Ces étapes sont indispensables à la mise en place de solutions adaptées et efficaces. À l'instar de Cornish (1994, p. 155), nous croyons qu'il est important de ne pas simplifier le processus dans lequel s'inscrit une activité criminelle, car seule une compréhension en profondeur des spécificités permet la mise en place de solutions adaptées et efficaces.

5. LES LIMITES DE LA RECHERCHE

Au même titre que plusieurs autres recherches, il importe de soulever certaines limites à notre étude. D'entrée de jeu, nous sommes conscients que nous possédons seulement cinquante pour cent (50%) de l'interaction entre les agents et les fraudeurs. Il faut donc être prudent sur les interprétations de l'interaction entre les protagonistes. De plus, il importe de prendre conscience que les données utilisées dans cette recherche, que ce soit les entretiens ou la base de données, portent sur les tentatives les plus faciles à identifier. On peut supposer que les fraudeurs les plus compétents ne sont pas dans les données analysées.

Ensuite, l'une des limites de notre recherche a trait à la mémoire des agents. Il ne fait aucun doute que les agents peuvent facilement discuter de leur environnement de travail, mais les informations sont limitées lorsqu'il s'agit de la description précise des tentatives non autorisées d'obtention de renseignements personnels. La qualité de l'information dépend de la capacité des agents à se rappeler les détails des situations vécues. Ces informations sont d'autant plus difficiles à trouver que les situations se sont généralement déroulées il y a plusieurs semaines, voire des mois, et que les tentatives non autorisées sont des situations atypiques. Cependant, cette faiblesse est en partie comblée par les rapports d'événements complétés par les agents à la suite de chaque tentative.

Par la suite, il est possible que le contexte des entretiens ait des répercussions sur le discours des agents (Poupart, 1997). Bien que les agents aient été informés que tous les éléments mentionnés lors des entretiens sont confidentiels et que nous ferions un usage scientifique exclusif de

l’information, il est possible que les agents aient perçu notre rencontre comme une évaluation et que leur discours diffère de la réalité. En d’autres mots, les agents auraient adopté un discours normatif. Pour pallier à ce risque, nous les avons informés que ces entrevues ne sont pas réalisées pour l’organisme public et qu’aucun suivi ne sera effectué individuellement avec le personnel. De plus, lors des entretiens, nous avons utilisé différentes stratégies d’écoute active afin de laisser le maximum de place à l’agent et de faciliter son discours.

Enfin, nous sommes conscients que notre échantillon n’a pas été créé de façon aléatoire. Nous avons dû le constituer par l’intermédiaire de la directrice adjointe ce qui peut introduire un certain biais. De plus, bien que la taille de notre échantillon soit suffisante dans le cadre de ce mémoire, il nous sera impossible de dresser un portrait rigoureux du phénomène pour toutes les organisations. Il est fort probable que le potentiel de généralisation des résultats soit limité aux centres d’appel. Toutefois, cette étude permettra d’améliorer les connaissances sur le sujet et apportera un support empirique intéressant.

CHAPITRE III :

LES RÉSULTATS

1. LES PROCÉDURES ADMINISTRATIVES

1.1. Le protocole d'identification

Afin d'être en mesure de comprendre le phénomène d'obtention non autorisée de renseignements personnels, il est nécessaire de décrire les principales procédures administratives en lien avec la protection des renseignements personnels de la clientèle. Donc, dans les prochains paragraphes, nous décrirons les deux principales mesures en place dans l'organisation soit le protocole d'identification et le processus de signalement.

En vertu des lois[31] en vigueur, toute personne qui travaille dans l'organisation a une obligation de discrétion et de confidentialité envers la clientèle utilisant ses services. Ainsi, tout le personnel a la responsabilité d'appliquer le protocole d'identification avant de transmettre toute information demandée lors d'un appel, d'une visite, d'un message télécopié ou d'un courriel. Si la personne n'a pu convaincre l'agent de son identité, elle sera avisée que l'information ne peut lui être transmise. Pour obtenir de l'information sur le dossier, le client doit être en mesure de confirmer un minimum de trois identifiants parmi un groupe de 6 éléments identificateurs[32]. Parmi le groupe obligatoire, nous retrouvons un code d'accès composé de numéros aléatoires qui est envoyé mensuellement à la clientèle et un numéro de dossier. Celui-ci est unique à chaque personne au même titre que le numéro d'assurance sociale et il composé de chiffres et de lettres. Le numéro d'assurance maladie et le nombre total d'enfants sont également des éléments du groupe obligatoire.

Normalement, le client devrait confirmer 3 éléments parmi les six obligatoires. Mais, si pour diverses raisons, les informations du groupe obligatoire ne sont pas au dossier ou que le client ne peut les fournir, l'agent a la possibilité d'utiliser les éléments du groupe complémentaire.

---

[31] Loi sur l'administration publique (L.R.Q., c. A-6.01) ; Loi d'accès aux documents d'organismes publics et protection des renseignements personnels (L.R.Q., c. A-2.1); Loi concernant le cadre juridique des technologies de l'information (L.R.Q., c. C-1.1) ; Loi sur la sécurité dans les édifices publics (L.R.Q., c. S-3) ; Charte des droits et libertés de la personne (L.R.Q., c. C-12, art. 5 et 44) ; Code civil du Québec, (art. 37 à 41); Directive sur la sécurité de l'information gouvernementale (C.T. 203560); Règlement sur la diffusion d'information et la protection des renseignements personnels (décret 408-2008, art.7).

[32] Pour des raisons évidentes de sécurité, il nous est impossible de présenter en détail les identifiants nécessaires pour réussir le protocole d'identification.

Toutefois, même si le client parvient à confirmer trois éléments, l'agent a toujours la liberté de poser davantage de questions afin de bien s'assurer qu'il parle à la bonne personne.

Advenant le cas où le client ne mentionne pas les mêmes éléments que ceux inscrits au dossier, que celui-ci ne peut répondre aux questions ou que l'agent a des doutes sur son identité, il lui refuse l'accès au dossier. À ce moment, l'agent mentionne au client qu'il doit se présenter en personne à son unité administrative avec deux pièces d'identité et quelqu'un mettra à jour son dossier et répondra à ses questions.

Habituellement, les agents se contentent de dire que les informations fournies ne correspondent à aucun dossier de l'organisation. En réalité, les agents accèdent rapidement au dossier du client en effectuant une recherche à l'aide du numéro de dossier, du NAM, du NAS ou du nom. Aussitôt les premières informations fournies par le client, l'agent bascule d'une fiche à l'autre afin de trouver les informations qui seront pertinentes pour le protocole d'identification. En prenant soin d'écouter la réponse du client, il doit regarder quelles autres questions il pourrait poser.

Dans la mesure du possible, les agents doivent tenter de varier les éléments du protocole d'identification afin que celui-ci ne soit pas répétitif et prévisible. En matière de sécurité, c'est ce que l'on appelle un protocole d'identification dynamique. Pour les agents, ce principe de changement continu est difficile à appliquer car une routine s'installe lors du protocole. De plus, ce principe est limité au nombre d'éléments présents dans le dossier du client. Dans les faits, nous avons remarqué que le protocole est peu dynamique.

Enfin, il importe de souligner que si une personne a réussi le protocole d'identification, mais que l'agent s'aperçoit au cours de l'appel, qu'elle n'est pas la personne qu'elle prétend être, l'agent mettra fin à la conversation et complétera une fiche de signalement. L'agent peut donc mettre fin à l'appel à n'importe quel moment de la conversation. L'agent peut également compléter une fiche de signalement si la personne n'a pas réussi le protocole d'identification, mais qu'elle a tenté d'obtenir des renseignements au dossier. En fait, la fiche doit être complétée même si la personne n'a pas réussi à obtenir de renseignements personnels.

1.2. Le processus de signalement

Afin d'être en mesure de collecter une quantité importante d'information sur les tentatives non autorisées d'obtention de renseignements personnels, l'organisme public a dû implanter une série de mesures et mobiliser plusieurs acteurs. L'organisme public a mandaté une direction qui contribue à l'élaboration et à l'évolution de la vision stratégique de l'organisation en tant que responsable du développement et de l'amélioration continue des mesures, des outils et des procédés requis pour assurer l'équité et la conformité dans la prestation de services. Cette direction occupe un rôle-conseil auprès des autorités de l'organisme public, et elle est, entre autres, responsable des tentatives non autorisées d'obtention de renseignements personnels.

Au sein de la direction, une seule personne est responsable de l'analyse et du traitement de l'information recueillie par les signalements. Cette dernière a développé un formulaire web, intitulé « Tentative d'accès non autorisée aux renseignements personnels», afin que les agents signalent à l'aide d'un outil uniforme les tentatives d'accès. La responsable des signalements est également chargée de la diffusion de l'information entre les différentes directions et du lancement d'alerte aux acteurs internes et externes clés.

Voici un court aperçu du processus de signalement dans son ensemble. Tout d'abord, les employés reçoivent une courte formation sur la protection de l'information et sont sensibilisés à l'importance de la confidentialité des informations au dossier du client. Au quotidien, lors de chaque appel, l'agent applique le protocole d'identification et s'il y a échec au protocole d'identification ou s'il a des doutes sur l'identité de la personne, il refuse l'accès à la personne et lui demande de se rendre dans une unité administrative pour obtenir des réponses à ses questions.

Lorsqu'un appel suspect est détecté, l'agent complète la fiche de signalement web et l'envoie à la responsable des tentatives d'accès non autorisées aux renseignements personnels de l'organisme. Lors de la réception de la fiche, cette dernière est lue et immédiatement ajoutée à la base de données centralisée. Si des détails pertinents à des analyses ultérieures peuvent être ajoutés à la fiche, la responsable effectue les modifications nécessaires. Advenant le cas où des renseignements personnels ont été communiqués sans droit à une tierce personne, la fiche est

identifiée d'une manière particulière et la responsable de l'application de la Loi de l'accès et de la protection des renseignements personnels est informée de la situation.

Ensuite, si le signalement contient assez d'information, il est examiné plus en profondeur. Les éléments tels que l'itinéraire de l'individu associé à plusieurs appels; les particularités du client cible et de l'individu; les stratagèmes utilisés; les doutes/indices de fraude malgré un protocole réussi; l'unité administrative locale ou centrale ciblée à répétition sont analysés. Par la suite, des croisements d'information sont effectués avec les autres signalements pour tenter d'identifier des personnes ou des établissements à risque.

À la suite de cette analyse, une alerte courriel peut être envoyée aux agents des centres d'appel si la situation l'exige. Par exemple, s'il y a eu plusieurs tentatives sur le même dossier dans une courte période de temps ou s'il y a un cas particulier qui mérite d'être connu de tous les agents. Si le signalement ne concerne pas l'échec au protocole, mais plutôt un comportement douteux contenant suffisamment d'indications sur l'appelant pour représenter un risque réel ou potentiel pour l'organisme, différentes instances et organisations externes sont contactées. Finalement, le processus de signalement tel que constitué ne prévoit pas que le client soit informé de la perte de renseignements personnels le concernant.

1.3. La liberté de l'agent

Maintenant que les deux principales mesures de sécurité sont décrites, nous croyons qu'il est important d'apporter quelques nuances quant à l'application de celles-ci. En effet, l'application de ces dernières repose sur une prémisse centrale, l'agent a une grande liberté d'action. Tout d'abord, nous retrouvons cette liberté dans l'application de protocole. S'il ne fait aucun doute que le protocole est toujours appliqué, les agents décident de la rigueur avec laquelle ils l'appliqueront. Par exemple, un agent peut demander le minimum de questions même s'il y a des signes qui porteraient à croire qu'il ne s'agit pas de la bonne personne. Un agent peut également décider de demander toujours les trois mêmes éléments.

Dans un second temps, lorsqu'un agent détecte une tentative non autorisée d'obtention de renseignements personnels, il est possible qu'il préfère ne pas remplir la fiche de signalement et passer à un appel suivant. Selon les agents rencontrés lors des entrevus, différentes raisons peuvent motiver un agent à agir ainsi. Il peut ne pas vouloir remplir la fiche de signalement, car cela demande plusieurs minutes et nuit à ses statistiques. Certains se disent qu'aucun renseignement n'a été communiqué donc cela ne donne rien. D'autres peuvent ne pas vouloir avouer qu'ils ont commis une erreur et préfèrent ne rien signaler. Dans les faits, si les agents du centre d'appel n'identifient pas des appels suspects, il y a peu de chance que l'organisation réalise qu'il y a des tentatives, car les conséquences sont indirectes pour l'organisation. En fait, on remarque que, dans son ensemble, le programme est basé sur le fait que l'agent prend la responsabilité de protéger les renseignements personnels et d'informer les autorités compétentes de l'organisme de tous appels suspects.

2. L'AMPLEUR DU PHÉNOMÈNE

L'objectif de cette section est de présenter les particularités de cette pratique frauduleuse. Afin d'atteindre cet objectif, nous présenterons dans un premier temps, un portrait sommaire des statistiques compilées par l'organisme public entre 2006 et 2010 en matière de tentatives non autorisées d'obtention de renseignements personnels. En plus de permettre d'évaluer l'ampleur du phénomène pour l'organisation, cette première étape nous permettra d'identifier les caractéristiques globales du phénomène. Par la suite, nous exposerons les détails du cas Martine, cette dame qui fût arrêtée par un service de police. Ce cas particulièrement riche en information constitue l'exemple le plus documenté à ce jour.

2.1. La fréquence des tentatives non autorisées d'obtention de renseignements personnels

Entre 2006 et 2009, un total de 1 110[33] tentatives ont été documentés par les agents de l'organisme public. Comme l'illustre le graphique 1, le nombre de signalements de tentatives non autorisées d'obtention de renseignements personnels est en constante augmentation depuis 2006.

---

[33] Afin de simplifier la présentation des données, nous avons seulement analysé les informations quantitatives collectés entre le 1er janvier 2006 et le 31 décembre 2009. Cependant, pour l'analyse des descriptions contenues dans les fiches de signalement, nous avons considéré la période entre le 1er avril 2006 et le 1er avril 2010.

Ainsi, nous pouvons observer que le nombre annuel de signalements est passé de 192 en 2006 à 367 en 2009, une augmentation de 186 %.

Graphique 1. Nombre annuel de signalements de tentatives non autorisées d'obtention de renseignements personnels entre 2006 et 2009.

Évidemment, il est possible d'attribuer cette évolution à un nombre de plus en plus élevé de tentatives. Cependant, considérant que le programme de signalement est en place depuis seulement 4 ans, l'interprétation de cette tendance doit être plus nuancée. En effet, il est possible que le nombre de tentatives ait toujours été à un niveau élevé, mais que la mise en place de la fiche numérique et du processus de signalement ait permis de mettre à jour graduellement le phénomène. Cela pourrait faire en sorte que l'on observe une évolution artificielle du nombre de tentatives.

L'augmentation constante des signalements présentée dans le graphique 1 pourrait également être attribuée à une plus grande sensibilisation et une meilleure formation des agents dans la détection des tentatives ainsi qu'à une amélioration des outils de signalement. Les statistiques pourraient donc indiquer un changement dans le travail et les perceptions des agents face au phénomène. Par conséquent, une amélioration des dispositifs entourant la détection expliquerait cette augmentation. Bref, il est difficile de dire si la tendance illustrée par le graphique 1 est due à l'augmentation effective des tentatives d'obtention de renseignements personnels ou à une amélioration de la détection des appels suspects. Bien que ces interprétations soient divergentes, elles ne remettent pas en doute la présence du phénomène.

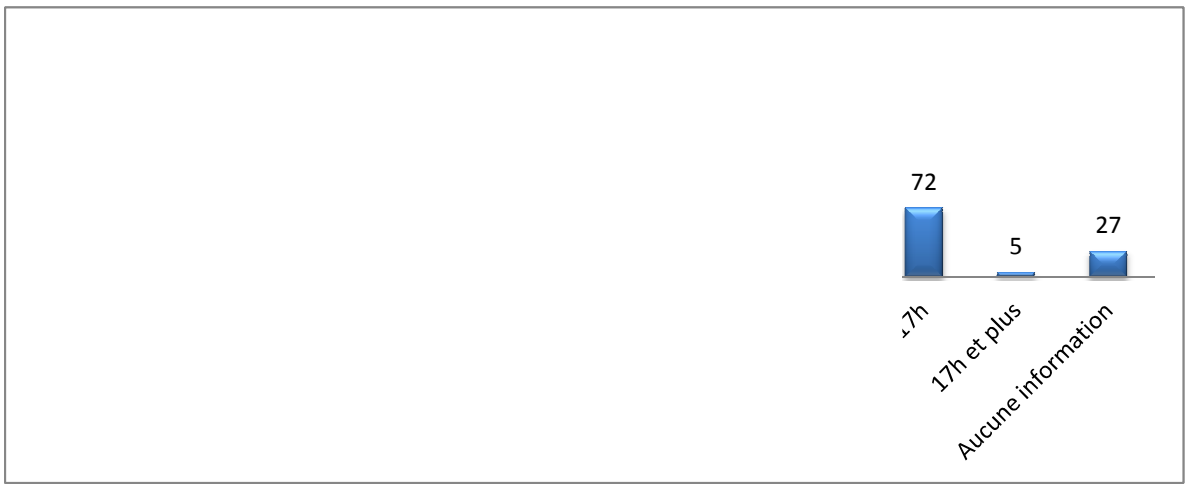
S'il ne fait aucun doute que les tentatives d'obtention sont un phénomène récurrent pour l'organisation, il est nécessaire de mettre en perspective le volume total de signalements. En effet,

les agents des centres d'appel répondent à environ cinquante (50) appels par quart de huit heures de travail. Or, en moyenne, selon nos entretiens, les agents disent croire qu'une personne tente d'obtenir des renseignements personnels lors d'un appel par semaine, soit environ un appel sur deux cents (200). Bref, une tentative est un événement atypique et si le volume total de signalements semble a priori impressionnant, il est nécessaire de le mettre en perspective dans le contexte de travail de l'agent.

À l'aide des statistiques, deux autres analyses descriptives ont été effectuées. Tout d'abord, nous avons analysé la fréquence des signalements pour chaque mois de l'année. Le nombre moyen de signalements pour les quatre années varie entre 52 et 165 avec une moyenne de 92,5 signalements par mois. Hormis les mois d'octobre, novembre et décembre qui ont totalisé un nombre plus élevé avec une moyenne de 132 signalements, aucune tendance n'est présente dans le graphique. Bien que les mois de juin, juillet et août soient plus propices à un roulement de personnel inhabituel en raison des vacances, ils ne semblent pas davantage ciblés par les présumés fraudeurs. Ensuite, nous avons analysé la répartition des signalements en fonction des jours du mois. Seuls les 1er, 2 et 28 de chaque mois ont une moyenne plus élevée que les autres jours. Ces résultats peuvent être attribués à un nombre plus élevé d'appels au début et à la fin de chaque mois.

Finalement, le graphique 2 illustre la distribution des signalements en fonction des heures de la journée. D'entrée de jeu, rappelons que la majorité des centres d'appel sont ouverts de 8 h 30 à 17 h. Selon le graphique, les périodes les moins ciblées semblent être tôt le matin, l'heure du dîner et en fin de journée. Un volume sensiblement égal a lieu de 9 h à 12 h (458 signalements) et de 13 h à 16 h (445 signalements).

Graphique 2. Fréquence des signalements de tentatives illégales d'obtention de renseignements personnels en fonction de l'heure.



Ce constat est intéressant dans la mesure où nous aurions pu croire que les présumés fraudeurs cibleraient davantage des moments où les agents sont moins attentionnés soit tôt le matin, l'heure de dîner et en fin de journée. Or, selon les données disponibles, les présumés fraudeurs ne semblent pas cibler particulièrement un moment précis de la journée. Ceci pourrait s'expliquer par le fait que les personnes qui cherchent à obtenir des renseignements personnels sur une personne le font dans un cadre professionnel. C'est-à-dire qu'ils passent leur journée (8 h et 17 h) à communiquer avec différentes organisations pour obtenir l'information désirée.

Ainsi, nous pouvons retenir que le nombre de signalements de tentatives d'obtention de renseignements personnels semble en constante augmentation depuis quatre ans. Ce volume élevé de tentatives détectées est surprenant dans une certaine mesure, car bien des organisations ont tendance à croire qu'il s'agit d'événements isolés alors que la mise en place d'un processus de signalement et de la collecte des informations sur les tentatives pourraient démontrer le contraire. En fait, la récurrence des tentatives non autorisées observée dans les analyses présentées procure des arguments tangibles démontrant qu'il s'agit d'une menace réelle à la protection de l'information. Cependant, bien que le volume total soit élevé, les tentatives demeurent des événements atypiques dans le quotidien des agents. Une analyse plus en profondeur des tentatives est nécessaire afin de mieux comprendre comment les présumés fraudeurs tentent d'obtenir des renseignements confidentiels et comment les agents les détectent.

2.2. Un exemple complet : le cas Martine

Afin d'analyser les tactiques utilisées par les présumés fraudeurs, nous débuterons par présenter un dossier fortement documenté par l'organisme public, celui nommé le cas Martine. Pour résumer les faits, la responsable des tentatives non autorisées d'obtention de renseignements personnels a constitué un dossier d'enquête à l'aide des informations contenues dans les fiches de signalement. Une fois le dossier bien étoffé de plusieurs signalements, celui-ci a été remis à la police qui a lancé son enquête pour finalement arrêter la dame en septembre 2009. Cette dernière a plaidé coupable à l'accusation de supposition intentionnelle de personne[34]. Elle a écopé d'une peine avec sursis dont la probation est de 3 ans et d'une amande de 600 $. Même si Martine possédait des antécédents en semblable matière, le juge a préféré lui donner une sentence avec sursis. Ainsi, la sentence, qui n'a pas été prononcée dans le cas de Martine, sera appliquée seulement si elle manque à ses obligations en récidivant.

Martine utilisait toujours le même stratagème. Elle appelait l'organisme public et se présentait comme étant une employée, d'une unité administrative d'une région quelconque. Dans la grande majorité des tentatives détectées, elle utilisait le nom de Martine Y, une employée réelle qui travaille effectivement dans l'organisation. Martine amorçait toutes les conversations de manière très amicale. Elle prenait le temps de se nommer et dire pour quelle unité administrative elle travaillait.

> "La madame était de bonne humeur et me parlait comme si elle était familière avec moi. Moi, vu qu'elle s'était nommée et dit de quelle unité administrative elle venait, je n'ai pas porté attention à sa demande. Je lui ai répondu normalement". (Signalement #108)

> "Elle agissait avec moi comme si je devais la connaître très bien et parlait qu'elle avait beaucoup de travail". (Signalement #125)

[34] Cette infraction faisant autrefois référence à l'article 403 du Code Criminel. Toutefois, le parlement canadien a adopté en janvier 2009 le projet de loi S-4 modifiant les infractions en lien avec le vol d'identité et inconduites connexes. Le projet de loi remplace la désignation de l'infraction actuelle de « supposition intentionnelle de personne » par la qualification de « fraude à l'identité » (art. 10 du projet de loi modifiant l'art. 403 du Code).

Selon les rapports des agents, elle était particulièrement dynamique, enjouée et sympathique. Martine prenait des nouvelles de la personne et de la température de la région. Par la suite, elle disait que son système informatique n'était plus fonctionnel depuis un moment, entre quelques heures et deux jours, et que les employés à son bureau ne comprenaient pas pourquoi. Tout le monde de son unité administrative devait alors travailler comme dans le bon vieux temps. Utilisant le prétexte de la panne de réseau, elle demande à l'agent de lui donner un coup de main parce que ce n'est vraiment pas facile de travailler sans l'informatique.

Une fois que l'agent a accepté de l'aider, Martine lui demandait si elle avait bien reçu le transfert du dossier physique d'un client. Évidemment, le dossier n'avait jamais été envoyé dans l'unité administrative en question. Ainsi, ne pouvant accéder au dossier de la personne par le réseau informatique, Martine demandait à l'employé si elle pouvait lui donner certaines informations, car elle n'était plus en possession du dossier physique. Martine possédait habituellement le nom, la date de naissance et le numéro d'assurance sociale de la personne. Le signalement #104 effectué le 18 novembre 2008 illustre bien le *modus operandi* de Martine :

> "Elle commence par me demander mon nom et je lui réponds. Elle se nomme, c'est Y de l'unité administrative 77. Elle me parle de la pluie et du beau temps de Montréal. Elle me demande si j'ai reçu en transfert le dossier de M. Sébastien D. Je vérifie dans le système informatique au nom de monsieur et aucun dossier dans notre secteur. Je lui dis non, mais elle me donne la date de naissance du client avec son numéro de dossier. Elle me dit que ça ne fonctionne pas quand elle le demande au système informatique. Je vérifie le numéro de dossier dans le système et je lui dis que j'ai le dossier et elle me demande s'il y a eu un changement dans son dossier concernant son adresse et je lui dis l'adresse et elle me dit HA! C'est bien bizarre ça, il n'a pas fait sa demande de transfert. Je lui dis qu'au niveau du système informatique, il n'y avait pas de demande de transfert. Elle me dit en tout cas, je vais te renvoyer le dossier. Je lui dis OK. J'ai déjà eu un appel de cette dame, il y a de ça un mois si ce n'est pas plus, et elle me demandait encore des informations dans un dossier qui déménageait à Chibougamau, mais encore une fois, il n'y avait aucun changement au niveau de l'adresse et aucun transfert n'avait pas été fait. (Signalement #104)

Cependant, dans la majorité des cas, l'employé contacté trouvait la demande étrange et il posait davantage de questions. Martine devenait alors vague et plus la conversation avançait, plus l'employé réalisait qu'elle agissait étrangement. Plusieurs employés lui ont alors demandé un numéro de téléphone pour la rejoindre. Dans ces cas, Martine précisait qu'elle ferait elle-même le suivi et qu'elle allait appeler le lendemain. Évidemment, les employés n'entendaient plus jamais

parler de Martine. Lorsque Martine réalisait que l'employé n'allait pas coopérer, il arrivait fréquemment qu'elle disait qu'elle allait effectuer une demande officielle de renseignement par télécopieur et que tout serait plus clair. Encore une fois, les employés n'ont jamais reçu de télécopie de la part de Martine. Enfin, il est arrivé à quelques reprises que Martine se sente piégée par une question et qu'elle raccroche la ligne. De plus, lorsqu'elle devait laisser un numéro de téléphone, elle laissait toujours un numéro de télécopieur pour ne pas soulever de soupçon.

2.3. Les stratégies et les motivations de Martine

Une analyse des fiches de signalement nous permet d'affirmer que Martine adoptait une approche sympathique afin de faciliter la collaboration de l'employé. En se nommant et en précisant qu'elle travaillait pour une unité administrative de même niveau, elle cherchait à établir rapidement un lien de confiance. Elle utilisait parfois des éléments de l'actualité telle que la météo pour créer un lien plus rapidement. De plus, Martine connaissait bien le langage, les termes utilisés ainsi que le fonctionnement de l'organisation. Il est possible qu'elle ait déjà travaillé dans l'organisation ou qu'elle connaisse bien quelqu'un qui y travaille. Il se peut également qu'elle ait déjà fait partie de la clientèle et que ses communications lui aient fourni le langage opérationnel nécessaire. De plus, les nombreuses informations disponibles sur Internet et les tentatives répétées qu'elle a effectuées lui ont probablement permis de bien comprendre comment fonctionne cet organisme public.

En analysant le cas Martine, on remarque qu'il y a beaucoup de rigueur et peu de place à l'improvisation dans ses tentatives. On pourrait dire que Martine a un scénario prédéterminé et bien travaillé auquel elle ne déroge presque pas. Considérant que le succès de Martine est relativement élevé comparativement à toutes les autres tentatives, nous croyons qu'elle constitue un exemple clair qu'une personne préparée et structurée peut obtenir des informations confidentielles dans de nombreuses organisations même si celles-ci ont implanté différentes mesures de sécurité.

Donc, Martine procédait systématiquement de la même manière en entrant en contact avec plusieurs unités administratives différentes. L'enquête de l'organisation a révélé qu'elle communiquait avec chaque région administrative du Québec jusqu'à ce qu'un bureau lui dise que

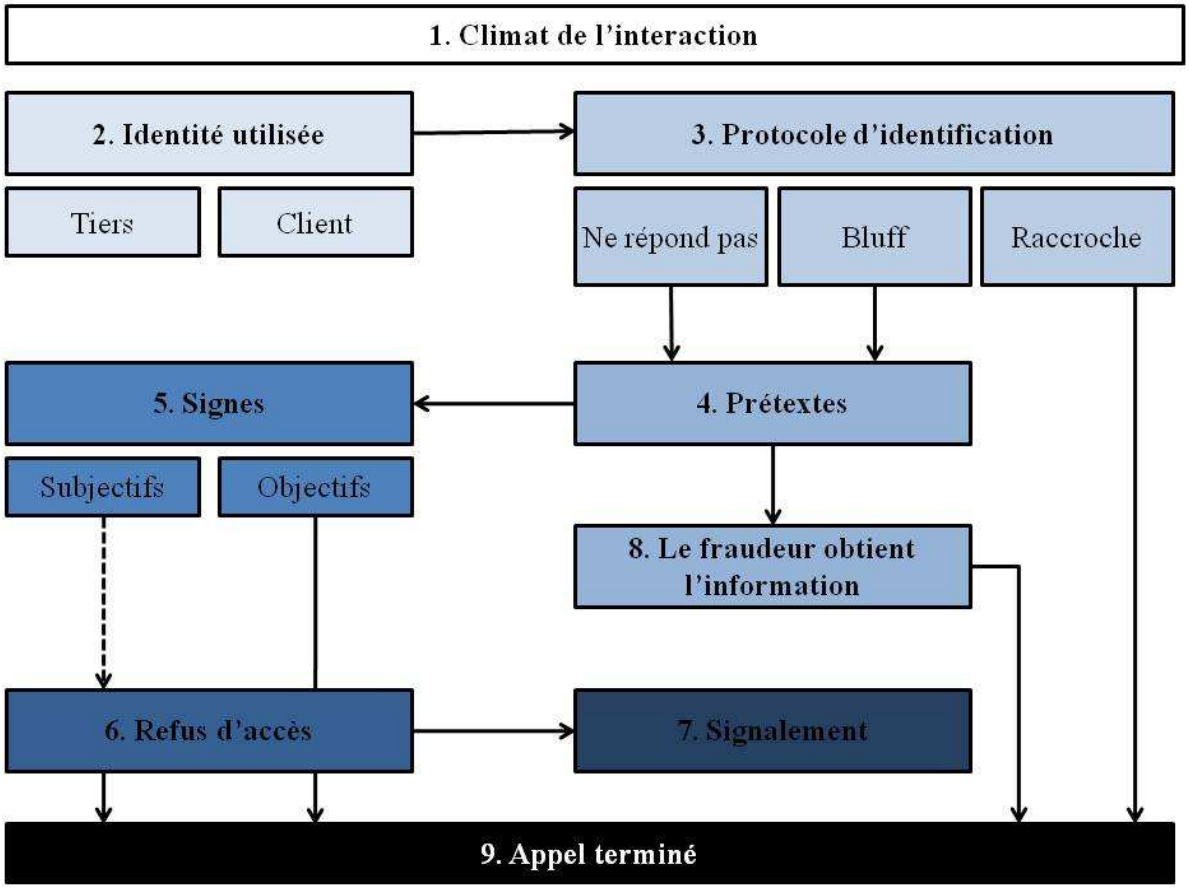
le dossier est effectivement dans cette région. À l'aide des signalements, il a été possible d'établir l'itinéraire des tentatives et de comprendre que Martine appelait plusieurs régions pour le même dossier. Dans tous les cas, Martine cherchait à obtenir l'adresse de la personne. Au total, après plusieurs années de collectes d'information, l'organisation a été en mesure d'associer soixante-dix (70) tentatives d'obtention à Martine. Les relevés de téléphone de Martine ont permis à la police de constater qu'elle exploitait également plusieurs autres sources telles que des sociétés de transport en commun, des banques, des pharmacies et des services de police. Selon l'enquête de la Sûreté du Québec, Martine effectuait les recherches pour des firmes d'avocat, des prêteurs usuraires et des agences de recouvrement. On peut déduire que ces tierces personnes demandaient à Martine de retrouver des personnes en particulier et cela, peu importe, les moyens utilisés. Martine était alors payée pour les informations qu'elle parvenait à collecter. Ainsi, on peut croire que ses principales motivations étaient économiques. Le cas de Martine nous illustre bien qu'il est possible que des gens travaillant dans des organisations légitimes aient recours à une tierce personne utilisant des moyens illégaux pour effectuer les recherches.

3. La Séquence d'interaction entre les acteurs

Dans cette troisième section, nous analyserons en profondeur la forme que prennent les tentatives non autorisées d'obtention en identifiant les tactiques criminelles utilisées lors de la majorité des tentatives. Nous entendons par tactiques criminelles, la séquence des choix et gestes posés par le délinquant durant les faits : la manière dont il combine les moyens disponibles pour réaliser ses fins tout en s'adaptant aux circonstances (Cusson & Cordeau, 1994, p. 13). Afin de décrire en détail les tentatives, nous présenterons un schéma développé illustrant l'interaction entre le présumé fraudeur et l'agent. En fait, l'analyse des fiches de signalement nous a permis de dégager neuf étapes qui rythment le déroulement de l'interaction entre le fraudeur et l'agent. Évidemment, toutes les tentatives d'accès ne contiennent pas systématiquement l'ensemble des étapes et elles ne sont pas toutes présentes dans le même ordre. Cependant, cette conceptualisation de la chronologie des événements est représentative dans la grande majorité des cas et elle nous permet de bien identifier les particularités de chaque étape. Ainsi, nous cherchons à répondre à la question suivante : Comment les délinquants exécutent-ils leur délit afin d'obtenir des renseignements personnels ?

En analysant chacune des séquences, nous parviendrons à comprendre concrètement les tentatives non autorisées d'obtention de renseignements personnels. Le lecteur notera que les étapes s'enchaînent selon une logique temporelle. La durée des étapes varie selon les cas, car elles sont influencées par différents facteurs, dont les actions et les réactions des acteurs. En fait, l'enchaînement des étapes est le résultat de l'interaction entre les deux protagonistes qui s'adaptent aux questions et aux relances de chacun. La figure 1 illustre la conceptualisation de la séquence de fraudes selon les informations recueillies par cet organisme public.

Figure 1. La séquence d'interaction entre le présumé fraudeur et l'agent des centres d'appel



La première étape représente le climat de l'interaction entre les protagonistes. Ensuite, les étapes 2, 3 et 4 mettent l'accent sur le fraudeur et les tactiques qu'il met en place pour obtenir l'information. Dans un premier temps, nous identifierons quelles sont les identités utilisées par le fraudeur. Ensuite, nous catégoriserons les prétextes invoqués par les fraudeurs selon leur nature.

De plus, nous identifierons les renseignements connus par le présumé fraudeur lors des tentatives. Lors de l'étape 4, nous analyserons le déroulement de l'interaction lorsque la principale mesure de sécurité, le protocole d'identification, est appliquée. Par la suite, lors des étapes identifiées 5 et 6, l'attention sera tournée sur le travail de l'agent alors que nous aborderons la détection des appels suspects. Nous enchaînerons avec la cinquième étape qui se produit lorsque l'agent a de sérieux doutes sur l'identité de la personne avec laquelle il discute. Nous identifierons les habilités développées par les agents pour reconnaître les appels frauduleux et sur les signes concrets disponibles pour les agents. La sixième étape survient lorsque l'agent refuse de divulguer l'information à la personne. Ainsi, dans cette section, nous aborderons la manière dont l'accès est refusé et la réaction du présumé fraudeur. Enfin, les étapes 7, 8 et 9 portent sur les dernières minutes de l'appel.

3.1. Le climat de l'interaction

Dans le contexte des tentatives non autorisées d'obtention de renseignements personnels, nous considérons l'attitude du présumé fraudeur comme le reflet du climat général de l'interaction entre ce dernier et l'agent. À ce sujet, les signalements révèlent que dans 58 % des cas de signalement, soit 642 cas, l'interlocuteur avait une attitude agressive par son langage ou son comportement lors de l'appel. Cette attitude peut se traduire par des injures, des cris ou des blasphèmes. La personne peut aussi adopter un comportement inadéquat en insistant et en mettant de la pression, en étant arrogante ou en refusant simplement de collaborer et de répondre aux questions de l'agent.

> "Monsieur dit qu'il appelle pour régler sa dette. Monsieur demande que je trouve son dossier avec son numéro d'assurance maladie. Monsieur supplie. J'insiste pour le NAS et le numéro de dossier. Les deux sont erronés. Monsieur tente de me distraire en parlant de la température. Comme je n'ai pas accès au dossier, monsieur se fâche et crie. Il demande mon nom. Il dit qu'il va porter plainte, car j'ai insinué qu'il tentait d'obtenir de l'information dans un dossier qui ne lui appartenait pas". (Signalement #87)

Quant au 42 % restant des signalements, les présumés fraudeurs adoptent une attitude plus sympathique. Ils sont aimables pour tenter de créer une ambiance favorable à la création de lien avec l'agent. La meilleure figure disponible est certainement l'exemple du cas de Martine. Nous

avons remarqué qu'il est possible d'identifier une troisième attitude. En effet, plusieurs appels se traduisent par une pression qui crée un sentiment d'urgence, mais qui ne met pas une pression indue sur l'agent. Cette catégorie se situe entre les deux catégories présentées précédemment et se traduit par insistance de la part du fraudeur, mais tout en demeurant respectueux.

Cette première section nous a permis de réaliser que les agents subissent fréquemment de la pression lors des appels. Cette attitude peut avoir pour objectif de repousser les limites de l'agent, car le fraudeur sait que l'agent peut régler cette situation désagréable en donnant simplement l'information demandée. Cette déstabilisation émotive fait en sorte que l'agent désire être plus gentil et se racheter en donnant au client ce qu'il désire. Cependant, en analysant seulement les tentatives non autorisées où des renseignements ont été obtenus, on réalise qu'être agressif ne semble pas être le moyen le plus efficace d'obtenir des renseignements personnels. En effet, il semble que les agents ont tendance à bloquer plus rapidement l'accès lorsqu'une personne devient agressive. À l'inverse, il semble qu'une attitude sympathique facilite les demandes de renseignement et augmente les chances de succès.

3.2. L'identité utilisée

En analysant la base de signalement, nous avons été en mesure d'identifier différentes identités utilisées par les présumés fraudeurs. En fait, plus de quatorze (14) identités ont été identifiées et nous les avons regroupées en deux grandes catégories. La première catégorie comprend les tentatives où le fraudeur prétend être le client alors que dans la seconde, le fraudeur se fait passer pour une tierce personne pouvant avoir légitimement accès au dossier du client. Ces deux stratégies, bien différentes, utilisent essentiellement les mêmes techniques de manipulation.

Selon les statistiques compilées, l'identité la plus fréquemment utilisée est celle du client. Ainsi, la majorité des tentatives, soit 84,5% implique des présumés fraudeurs qui prétendent être le client de l'organisme. Les autres identités utilisées impliquant des tierces personnes représentent 15,5 %, soit 182 cas. À l'intérieur des 182 cas, 43,1 % sont des personnes qui se faisaient passer pour un employé de l'organisation, 24,6 % pour un intervenant (psychologue, travailleur social, avocat, policier) et 32,3 % pour un membre de la famille (parent, frère, sœur).

Ainsi, on remarque que les fraudeurs prétendent être davantage le client qu'une tierce personne. Cette stratégie consistant à utiliser l'identité du client peut signifier que les fraudeurs croient qu'il est plus facile d'obtenir des informations au dossier en prétendant être le client, car le dossier lui appartient. De plus, les fraudeurs croient peut être qu'il est plus simple de se faire passer pour le client que de se faire passer pour un policier ou un avocat, car ces derniers possèdent des connaissances particulières et emploient un langage particulier.

En ce qui concerne l'utilisation de l'identité d'une tierce personne (n=167), l'un des éléments les plus marquants est certes l'utilisation de l'identité d'un employé de l'organisation. Pour être efficace, cette stratégie demande une bonne connaissance du milieu. Cependant, il importe de noter que dans les 72 cas signalés, la presque totalité est reliée au cas de Martine présenté plus tôt. Ainsi, depuis son arrestation, le nombre de tentatives impliquant un employé a considérablement diminué. Cependant, comme nous l'indique le signalement #192, cette stratégie est toujours possible. En effet, dans le signalement suivant, le fraudeur a prétendu être un employé d'une unité de l'organisation :

> "La personne téléphone et s'identifie comme enquêteur au centre W (Daniel O.). Il nomme le client et dit que cette personne n'est pas conforme. Il dit qu'il veut vérifier certains renseignements et demande de confirmer le numéro de client, ce que j'ai fait (il ne possédait pas cette info). Il dit qu'il veut des renseignements et je dis que je vais faire le message à l'agent que le client est sur le programme D. Quand je téléphone au numéro de téléphone laissé pour le retour d'appel (par l'enquêteur), le 514-580-2222, c'est le 911 qui répond et personne ne connaît M. Daniel O. à ce numéro de téléphone." (Signalement #192)

Au sein de ce groupe, les autres identités utilisées impliquent des intervenants de différents domaines. Nous les avons classés en deux groupes. Tout d'abord, il y a les identités qui ont un certain statut dans la société. Dans ce groupe, nous incluons les cas qui impliquent de prétendus policiers de la GRC, des avocats, des psychologues, une agente d'immigration Canada et un attaché politique. Les identités des policiers et des avocats sont certainement les plus fréquemment utilisées par les présumés fraudeurs. En adoptant cette identité, ils cherchent à tirer profit de la position sociale dont jouissent ces personnes. Ensuite, le deuxième groupe implique des personnes qui sont en contact direct avec la clientèle de l'organisation. Il s'agit de travailleur social, d'intervenant de centre de réhabilitation, d'agent d'intégration et de secrétaire. Dans l'exemple qui suit, une personne prétendant être une secrétaire d'une clinique dentaire disait avoir l'autorisation du client pour effectuer une transaction. Il est possible que si l'agent avait

communiqué avec la secrétaire, celle-ci aurait cherché à obtenir des renseignements personnels sur Mme C.

> "J’ai un message sur ma boîte vocale de rappeler Mme Christine P. de la Clinique 123 de Longueuil. Mme P. dit que Mme C. lui a dit de m'appeler et que je lui donnerais l'autorisation pour le paiement de soins dentaires reçus en septembre 2008. Je rappelle Mme P., lui laisse un message de me rappeler. Je fais entretemps une recherche avec le numéro de téléphone et l'information au 411. Le numéro est associé à l’Agence de recouvrement XY. " (Signalement #131)

Finalement, les autres cas impliquent des personnes qui prétendent être des membres de la famille (54 cas). Nous croyons que l’un des éléments qui différencie cette catégorie des autres est qu’il s’agit souvent de la réelle identité de la personne. En effet, d’après les signalements et les entretiens avec les agents, il est possible d’identifier la relation de la personne avec le client, car elle avoue d’elle-même ne pas être la personne qu’elle a prétendu être au début de la conversation. Dans cette catégorie, il s’agit souvent des personnes qui tentent d’aider un membre de la famille. Cette interprétation est en résonance avec les commentaires des agents qui nous ont mentionné avoir l’impression, lorsqu’il s’agit d’une personne qui avoue être un membre de la famille, qu’elle voulait seulement aider le client. Dans ces situations, les agents nous ont mentionné qu’il était très rare qu’ils complètent une fiche de signalement, car ils ne voyaient aucune intention malicieuse dans la situation. Ainsi, il est intéressant de remarquer que lorsqu’une personne avoue avoir menti sur son identité, mais qu’elle mentionne être de la famille du client, la justification n’est pas remise en question par les agents et le doute sur la tentative non autorisée est écarté. Or, il est possible qu’un fraudeur qui tente d’obtenir de l’information prétende être un membre de la famille qui veut seulement aider afin de ne pas attirer de soupçon.

3.3. Le protocole d’identification

L’application du protocole mène systématiquement à une interaction particulièrement intéressante, car le fraudeur connaît plus ou moins les questions qui lui seront posées. Ainsi, il doit ajuster sa tactique, dans la mesure du possible, en fonction des questions de l’agent et des informations qu’il possède. Il doit également rester cohérent avec l’identité qu’il a adoptée au début de l’appel. Notre analyse nous a permis d’identifier trois trajectoires possibles pour le présumé fraudeur du protocole d’identification.

Tout d'abord, la première trajectoire observée implique que le présumé fraudeur ne peut pas répondre à la question du protocole. Par conséquent, il va utiliser des prétextes et différentes techniques de manipulation afin de détourner l'attention de l'agent et gagner du temps. Les prétextes utilisés ainsi que les techniques de manipulation seront développés plus en profondeur dans les prochaines pages.

Ensuite, lors de la seconde trajectoire, le présumé fraudeur invente une réponse. Cette stratégie, beaucoup plus utilisée que l'on peut le croire, permet à ce dernier de démontrer de l'assurance dans ses réponses. Il arrive fréquemment que les présumés fraudeurs inventent une adresse, un numéro de téléphone ou le montant de la prestation. Pour l'agent, il est difficile de savoir si l'information fournie est la bonne ou non, car la mise à jour des informations au dossier client n'est pas toujours effectuée. Par contre, cette stratégie est risquée pour des informations comme le NAS et le NAM, le nombre d'enfants et le type de dépôt qui ne font presque jamais l'objet de modification.

Finalement, la troisième alternative, qui peut également se produire en combinaison avec les deux premières est que le présumé fraudeur quitte la ligne. Cette situation est présente dans de nombreux signalements et elle peut être interprétée de différentes manières. Tout d'abord, il peut s'agir d'un problème technique ou d'une erreur. Cependant, il est raisonnable de croire que lorsqu'une personne raccroche le téléphone lors du protocole d'identification, c'est qu'elle se sentait piégée et qu'elle ne pouvait répondre à la question. Pour les prochains paragraphes, nous allons développer les deux premières trajectoires que nous avons identifiées.

3.4. Les prétextes

Les prétextes utilisés par les fraudeurs sont certainement l'un des éléments intéressants que les fiches de signalement nous ont permis d'identifier. Rappelons-le, les prétextes sont des justifications inventées par le fraudeur pour obtenir de l'information. Ces justifications sont intimement liées au climat de la conversation, à l'identité utilisée par ce dernier et à l'application du protocole d'identification. Concrètement, ils permettent au fraudeur de justifier sa demande ou son incapacité à répondre à une ou plusieurs questions du protocole d'identification.

3.4.1. La nature des prétextes

La crédibilité du prétexte utilisé est assurément l'un des facteurs les plus déterminants de la tentative d'obtention. Plus le prétexte est convaincant et adapté au contexte, plus la demande d'information semblera légitime pour l'agent. Pour cette section, nous allons présenter les prétextes utilisés selon deux situations très fréquentes dans les signalements.

Tout d'abord, le fraudeur va créer une situation où l'agent peut régler un problème ou un souci. L'un des prétextes les plus fréquents est de dire à l'agent qu'il n'a pas reçu un document normalement transmis par l'organisme public. Il peut s'agir d'un formulaire, d'un carnet, d'un relevé ou d'une décision. Par la suite, le fraudeur demandera à l'agent à quelle adresse le document a été posté, car il ne l'a pas reçu. Lorsque l'agent lui demandera son adresse, le fraudeur donnera une adresse quelconque. En utilisant ce prétexte, le fraudeur cherche à connaître l'adresse exacte du client. Considérant que l'une des motivations les plus fréquentes est de retrouver une personne, nous avons remarqué que cette stratégie est particulièrement utilisée.

Ensuite, plusieurs fraudeurs appellent pour confirmer un changement d'adresse. Ils mentionnent qu'ils ont fait un changement d'adresse plus tôt dans la semaine et qu'ils désirent savoir si tout est en ordre. Évidemment, le changement d'adresse n'est pas effectué, car il n'a jamais eu lieu. Le fraudeur mentionnera une adresse ne figurant pas au dossier en prétendant que c'est la nouvelle adresse qu'il a donnée lors du dernier appel. Il fournira alors de nombreux détails concernant le dernier appel afin d'avoir l'air le plus crédible possible. Par la suite, le fraudeur cherchera à connaître l'adresse inscrite au dossier.

Nous avons remarqué que le même prétexte est applicable pour le numéro de téléphone. Le fraudeur prétend avoir changé de numéro de téléphone, mais l'objectif est de connaître l'ancien numéro. Nous avons également identifié d'autres situations plus particulières où l'aide de l'agent est sollicitée. Les problèmes informatiques du cas Martine sont évidemment un excellent exemple. Un autre cas intéressant est celui de cet individu prétendant être un avocat de l'organisation. Il affirmait devoir faire une vérification de routine sur le client afin d'éviter de le faire déplacer à la cour. Si l'agent communiquait les renseignements, l'organisme public épargnerait du temps et de l'argent. Dans ce signalement, l'agent a refusé l'accès et il a demandé à l'avocat de faire une demande en règle par écrit. Cette demande n'a jamais été effectuée. Dans le même ordre d'idées, un fraudeur s'est présenté comme un policier et désirait obtenir l'adresse

d’un client qui était considéré comme un fugitif. Encore une fois, l’agent a refusé de divulguer l’information et il a demandé d’acheminer une demande écrite. Encore une fois, aucune demande officielle n’a été reçue.

Le deuxième groupe de prétexte permet au fraudeur de justifier son incapacité de fournir certaines informations. Le prétexte le plus fréquemment utilisé par le fraudeur pour justifier une erreur dans l’adresse est de dire qu’il déménage souvent et qu’il ne se souvient pas de certaines informations. Le fraudeur va aussi dire qu’il est dans un lieu différent et qu’il ne peut pas avoir l’information pour le moment. Ainsi, plusieurs mentionnent appeler d’une cabine téléphonique, être chez un voisin, un ami ou dans une boutique. Ensuite, pour justifier l’incapacité de fournir une information, certains diront qu’ils ont perdu leur portefeuille, qu’ils ont été volés ou que leur maison a brûlé. Enfin, nous avons remarqué que certains fraudeurs mentionnent être sous médication pour justifier leur désorganisation ou l’incohérence dans leur propos.

Finalement, nous avons identifié un prétexte qui ne peut pas être classé dans les deux premiers groupes, mais qui mérite d’être mentionné. D’après les signalements et les propos des agents, les fraudeurs mentionnent fréquemment qu’ils viennent d’être transférés à un autre agent et que la personne avant lui a déjà posé toutes les questions d’identification.

Pour le fraudeur, les prétextes sont essentiels, car ils leur permettent d’éviter de répondre à certaines questions. Ainsi, il s’abstient de commettre une erreur qui compromettrait sa tentative. De plus, les prétextes leur permettent de gagner du temps en justifiant la confusion ou l’absence d’information. D’après tous les signalements que nous avons lus, les prétextes les plus efficaces sont ceux qui sont simples. Plus le fraudeur donne des détails sur sa situation, plus il a de chance de commettre une erreur et d’exposer les faiblesses de son scénario.

Nous avons également remarqué que dans la majorité des signalements, le choix du prétexte semble assez aléatoire dans la mesure où le fraudeur semble prévoir une ou deux relances possibles. Lorsque l’agent pose davantage de questions, le fraudeur ne peut pas répondre et sa demande devient de moins en moins légitime. En fait, la difficulté pour le fraudeur est d’inclure plusieurs solutions de rechange à l’intérieur de son prétexte tout en restant cohérent. Ainsi, pour les agents, plus il y a d’échanges lors de l’appel, plus ils ont de chance de détecter des signes suspects.

3.4.2. Les techniques d'ingénierie sociale

La littérature sur l'ingénierie sociale nous a permis d'identifier plusieurs techniques de manipulation utilisées dans différentes situations. Nos analyses nous ont permis d'identifier si ces stratégies sont également utilisées dans les tentatives non autorisées d'obtention de renseignements personnels.

Tout d'abord, l'une des techniques de manipulation qui semblent les plus efficaces est d'adopter une attitude sympathique pour tenter de créer un lien avec l'agent. Pour l'organisation en question, tous les cas où des renseignements ont été perdus impliquent ce type de situation. Ce constat rejoint les propos de Cialdini (1993) qui affirme que la meilleure manière de manipuler les gens est simplement d'être gentil. Par contre, comme l'interaction se déroule au téléphone, le fraudeur peut seulement utiliser le langage pour créer un lien avec l'agent. Notre analyse montre qu'ils parleront de la température et de la charge de travail au bureau. Ils vont également utiliser des formules de politesse telles que : "Je ne veux pas prendre trop de votre temps" ou "À qui ai-je l'honneur de parler? " En ce qui concerne le principe de la similarité, le meilleur exemple est certes celui du fraudeur qui prétend être un employé de l'organisation. Par contre, outre le lien qui est créé par l'appartenance à la même compagnie, nous n'avons pas pu dégager d'autres exemples concrets.

Ensuite, au niveau du principe de la réciprocité, qui veut que le simple fait de réaliser un acte des plus anodins prédispose une personne à accepter, plus favorablement, une requête ultérieure bien plus coûteuse en temps et en argent, nous avons remarqué que ce principe ne s'applique pas aux tentatives non autorisées d'obtention de renseignements personnels. Premièrement, parce que l'agent est en contrôle de l'appel. Il dirige l'interaction en choisissant les questions du protocole d'identification. Deuxièmement, contrairement à un vendeur, le fraudeur n'a pratiquement rien à offrir à l'agent. Ainsi, il ne peut pas créer le sentiment d'obligation qui accompagne l'acceptation de l'offre initiale. Il est difficile pour le présumé fraudeur de créer un sentiment que l'agent lui doit quelque chose. Par contre, il utilise une variante du principe lorsqu'ils disent à l'agent qu'ils veulent juste savoir un élément simple au dossier. Les fraudeurs misent alors sur le fait que la demande est minime et que l'agent ne verra pas de conséquence à transmettre cette information.

Par la suite, l'une des techniques utilisées consiste à dire que les autres agents ne lui ont jamais posé cette question ou que le protocole n'a jamais été aussi complexe. En utilisant le principe de la preuve sociale, les fraudeurs espèrent que l'agent adoptera le comportement du groupe. Par exemple, il dira que cela fait cinq ans qu'il appelle et qu'il donne toujours juste son nom, son adresse et son numéro de téléphone. Il pourra également dire que les autres agents ne lui posent jamais cette question. Si les agents entendent souvent ce type de réplique, elle semble avoir peu d'impact sur leur comportement.

La quatrième technique utilisée est certainement l'une des plus intéressantes. Les fraudeurs utilisent fréquemment l'autorité pour obtenir des renseignements personnels. Afin de créer cette figure d'autorité, les fraudeurs utilisent des titres professionnels et un langage spécifique. L'avocat et le policier sont certainement les deux figures les plus utilisées par les fraudeurs. Ils utilisent leur titre pour dire qu'ils ont légalement le droit d'avoir accès à l'information. D'après les agents, lorsqu'une personne se présente et qu'elle a un certain titre, cela influence leur comportement. Par exemple, un agent nous évoquait un appel où un attaché politique désirait obtenir de l'information sur le membre de la famille pour haut placé de l'organisation:

> "Elle m'a dit: Je suis l'attaché politique de monsieur K. On m'a dit que vous pouviez régler un problème. Là, j'avais un motton. Sais-tu vrai ? Mais, ça m'a allumé une lumière. Mais, elle était très professionnelle". (Entretien #7).

En fait, par cet exemple, on remarque que le simple fait de prétendre être quelqu'un qui a un titre influence le comportement de l'agent et la manière dont le protocole sera appliqué. Par contre, des agents nous ont mentionné que cette stratégie peut aussi avoir l'effet contraire. Ils nous ont dit qu'avec l'expérience, lorsqu'un avocat communique avec eux, ils font davantage attention et rendent le protocole plus difficile, car plusieurs cas frauduleux leur ont été rapportés.

Enfin, la dernière technique repose sur le facteur temps. Le facteur temps est utilisé par les fraudeurs afin de créer un besoin urgent d'aide. Ainsi, plusieurs fraudeurs mettent une pression significative sur l'agent pour qu'il règle leur problème immédiatement. Il arrive que des personnes très pressées demandent de faire le protocole plus rapidement parce qu'ils ne peuvent pas rester en ligne longtemps. Dans ces situations, l'attention de l'agent est mise sur le facteur temps et non sur la teneur de la demande. Par contre, nous n'avons pas de données sur le temps

d'appel des tentatives non autorisées. Ainsi, l'analyse des fiches de signalement n'a pas permis d'identifier si le facteur temps était utilisé par les fraudeurs. De plus, nous savons déjà que les fraudeurs ne ciblent pas un moment de la journée précis[35].

Nous pouvons retenir de cette section que la confiance est une pierre angulaire du succès des fraudes. Lorsque le fraudeur réussit à créer un lien avec l'agent, la probabilité qu'il obtienne ce qu'il désire est beaucoup plus élevée. Il est intéressant d'analyser comment cette confiance parvient à s'établir dans ce contexte temporel et organisationnel particulier. En fait, nous avons remarqué qu'en raison du temps très limité des conversations, le fraudeur doit chercher à créer un lien de confiance suffisant avec l'agent. Il n'est pas nécessaire pour le fraudeur de chercher à établir un lien solide avec l'agent, mais il doit plutôt miser sur des éléments simples comme adopter un langage commun, prendre des nouvelles de la personne et surtout être sympathique. Les recherches en psychologie cognitive ont démontré que l'humain prend plusieurs décisions fortement basées sur l'impression qui survient automatiquement et indépendamment de toute évaluation objective (Tversky & Kahneman, 1974). Si le fraudeur parvient à influencer cette impression dès le début de l'appel, cela peut jouer un rôle important dans la prise de décision de l'agent. Dans le contexte des centres d'appel, les constats de Tversky & Kahneman (1974) sont d'autant plus importants que les agents répondent à environ cinquante appels par jour et qu'ils leur soient impossible d'analyser toutes les informations qu'ils reçoivent. Ainsi, il est fort possible que l'impression laissée par le fraudeur joue un rôle important dans la prise de décision. De plus, le fraudeur profite d'un avantage important, car il peut tenter l'expérience sur plusieurs personnes. Ainsi, il peut répéter son stratagème jusqu'à ce qu'il discute avec un agent avec lequel il pourra créer un lien.

3.4.3. Les renseignements connus

Grâce aux fiches de signalement, il nous a été possible d'identifier les renseignements connus par les fraudeurs. À la suite d'une tentative, l'agent complète une section de la fiche de signalement où il peut indiquer les renseignements qui étaient connus par le fraudeur. Évidemment, les éléments qui sont mentionnés dépendent des questions qui sont posées par l'agent. Cependant, en analysant les signalements, on remarque que les fraudeurs vont généralement divulguer d'eux-mêmes les renseignements qu'ils connaissent pour paraître plus crédibles. En fait, il est

[35] Voir le graphique 2, page 78.

raisonnable de croire que le fraudeur mentionnera tous les renseignements qu'il connaît sur la personne pour tenter d'être le plus convaincant possible. Il est fréquent que les fraudeurs disent, je n'ai pas le NAM mais j'ai mon NAS ou je ne connais pas le numéro du dossier, mais je t'ai déjà donné mon nom et mon adresse, ça devrait suffire. Il est d'autant plus pertinent d'identifier les renseignements connus par le fraudeur, car ce sont ces éléments qui permettent au fraudeur de construire un prétexte crédible.

Tableau 3 : Les renseignements connus par les personnes lors des tentatives non autorisées d'obtention de renseignements personnels

	(n*) 1136	**%***
Nom et prénom	1055	92,9
Numéro de client	851	74,9
Adresse	648	57,0
Numéro de téléphone	489	43,0
Numéro d'assurance sociale	401	35,3
Date de naissance	394	34,7
Numéro d'assurance maladie	278	24,5
Autres	187	16,5
Montant de l'allocation	135	11,9
Dépôt direct	87	7,7
Nom des enfants	79	7,0
Nombre d'enfants	53	4,7
Réclamation existante	10	0,9

*Le (n) est plus élevé que le nombre de signalements, car il est possible que des agents aient coché plusieurs éléments pour la même tentative.

Le tableau 3 présente les renseignements connus par le fraudeur au moment de la tentative d'accès. On remarque que le nom (92,9 %) et le numéro du client (67,2 %) sont les deux éléments les plus connus du fraudeur. Par la suite, dans les cas signalés, 57 % connaissait l'adresse complète et 43 % le numéro de téléphone. Il est tout de même surprenant de constater que ces deux éléments de base ne sont pas davantage connus. Enfin, les informations concernant les enfants (11,7 %), le type de dépôt (7,7 %) et le numéro d'assurance maladie (24,5 %) semblent être moins connues.

3.5. Les signes

Dans les prochains paragraphes, nous aborderons les mécanismes de détection développés par les agents. Notre terrain de recherche est particulièrement intéressant pour la détection, car la grande majorité des signalements impliquent nécessairement des tentatives détectées. Nous avons donc identifié les éléments qui contribuent à la détection des tentatives non autorisées d'obtention de renseignements personnels. À la suite de notre analyse, nous avons divisé les signes en deux groupes, les signes objectifs et subjectifs. Cette dichotomie, bien qu'imparfaite, nous permet de faire la différence entre les habiletés développées par les agents et les indices que toute personne pourrait identifier. Alors que les signes subjectifs laissent place à beaucoup d'interprétation, les signes objectifs sont des indices concrets qui ne peuvent être remis en doute. Afin d'identifier les signes permettant la détection, nous avons utilisé à la fois les entretiens avec les agents et les fiches de signalement.

3.5.1. Les signes objectifs

Les signes objectifs sont donc des indices concrets qui permettent de détecter les tentatives non autorisées d'obtention de renseignements personnels. Notre analyse des fiches de signalement nous a permis de distinguer quatre signes objectifs qui permettent à l'agent de s'assurer qu'il s'agit d'une fraude. Tout d'abord, il arrive que lors de l'appel, l'interlocuteur passe soudainement de la première personne du singulier à la troisième personne. Cet élément, de changer soudainement le « je » par le « il » est fréquent et les agents le considèrent comme un point de rupture. Il est très rare qu'une personne va parler à la troisième personne et l'agent va profiter de cette erreur pour confronter la personne et lui demander si elle est bien la personne qu'elle prétend être. La plupart du temps, la réaction de la personne, qui comprend qu'elle a commis une erreur, confirme qu'elle n'est pas la personne qu'elle prétend être. Pour les agents, plus l'appel est long et plus il y a d'échanges avec la personne, plus il y a de chance que celle-ci commette ce type d'erreur.

Ensuite, il arrive que le fraudeur appelle concernant un dossier qui est fermé dans l'organisation. En effet, plusieurs signalements impliquent des personnes qui prétendent être un client de l'organisation alors que le dossier est fermé depuis plusieurs années. Il est aussi arrivé qu'une intervenante appelle au sujet du dossier d'une dame qui était décédée.

> "Elle se présente comme une intervenante et dit avoir une procuration au dossier. Elle veut savoir pourquoi elle (sa cliente) n'a pas reçu l'allocation de mai et se demande si c'est parce qu'elle a oublié de faire le changement d'adresse en février. Elle dit que sa cliente est déménagée le 21 février. Je n'ai pas vu de procuration au dossier au nom de Mme L. Elle ne savait pas que la cliente était décédée en mars. Elle n'a pas insisté pour avoir les renseignements après lui avoir dit que je n'avais pas accès au dossier. J'ai cependant trouvé bizarre qu'une intervenante ignore le décès de sa cliente et appelle pour savoir pourquoi elle n'avait pas eu allocation". (Signalement #83)

Par la suite, il arrive que les fraudeurs fournissent une mauvaise réponse à des questions personnelles. Pour l'agent, il est particulièrement intéressant de poser des questions personnelles car le fraudeur n'a pas le choix de donner une réponse, étant donné qu'il s'agit d'une information qu'il doit nécessairement connaître. Dans l'exemple qui suit, le fraudeur avait un NAS, mais il a donné la mauvaise date de naissance :

> "Monsieur appelle. Se présente et dit être Pascal B. Il dit ne pas avoir son numéro de dossier, mais il donne le NAS et on tombe dans le dossier d'un Pascal C. Il dit être né le 11 novembre 1965, alors que dans le dossier, l'année de naissance est 1969. Je dis à Monsieur que je n'accède pas au dossier. Il dit qu'il ne me croit pas. Je demande le numéro de téléphone pour rejoindre monsieur. Il me donne le 514-123-4567. Je fais ce numéro, mais sans réponse. C'est la 2^{e} fois que je tombe sur lui". (Signalement #25)

Alors que dans cette situation, la dame s'est trompée dans le nombre d'enfants :

> "En faisant le protocole d'identification, la date de naissance de notre cliente ne correspondait pas avec la date de naissance de l'interlocutrice. De plus, j'ai demandé s'il y avait des enfants au dossier et combien. Elle m'a répondu qu'elle en avait 4 alors qu'au dossier il y apparaît un enfant seulement. Comme les dates de naissance ne correspondaient pas, j'ai demandé le pourquoi de la différence pour la date de naissance? La personne m'a répondu qu'il y avait eu une erreur. Je lui ai demandé comment pouvait-il y avoir une erreur sur la date de naissance? La personne a raccroché". (Signalement #80)

Une autre question personnelle qui est intéressante pour les agents est le type de dépôt. Il y a deux types de dépôt, soit il est effectué par chèque, soit par dépôt direct. Lorsqu'il s'agit d'un dépôt direct, l'agent peut demander le numéro de compte bancaire ou le nom de l'institution financière. S'il est fréquent que la personne ne puisse pas donner par cœur son numéro de compte bancaire, il est beaucoup plus difficile pour une personne de justifier son incapacité à dire le nom de son institution financière. Dans la situation qui suit, un homme commet une erreur dans le type de dépôt ce qui permet à l'agent de détecter facilement la tentative:

> "Monsieur me dit qu'il n'a pas reçu son allocation par la poste. J'effectue le protocole d'identification, l'adresse ne concorde pas du tout. Je lui demande depuis combien de temps il demeure à cette adresse. Il me dit qu'il demeure à une adresse depuis 2 ans, et qu'il a toujours reçu son allocation à cette adresse. Je lui demande de passer directement avec des pièces d'identité au bureau. Il me répond attendez madame j'ai une autre adresse. Je lui répète de se présenter au bureau. En vérifiant le dossier, je constate qu'habituellement il reçoit sa prestation par dépôt direct". (Signalement #119)

Il ne fait aucun doute qu'une erreur dans le nombre d'enfants, la date de naissance du plus jeune et dans le nom de l'institution financière sont des preuves importantes pour l'agent qu'il ne parle pas à la bonne personne. La faiblesse de ce type de questions est que les membres de la famille connaissent généralement les réponses.

Le troisième élément est particulièrement intéressant, car il nous permet de confirmer que l'appel était une fraude. Il arrive pour diverses raisons que l'agent demande un numéro de téléphone à rappeler, car il a des doutes concernant la demande ou il n'est pas en mesure de répondre immédiatement à une question. Cette pratique d'appeler le numéro de la personne inscrite au dossier, appelée procédure de rappel[36], est fréquemment utilisée dans les services bancaires lorsque les agents au service à la clientèle croient qu'il s'agit d'une fraude. Par conséquent, il communique avec le client pour confirmer qu'il est bien entré en contact avec l'établissement quelques minutes auparavant. En analysant les signalements, nous avons identifié neuf (9) cas où l'agent a effectué un retour d'appel. Dans tous les cas, soit le numéro était invalide ou la personne qui répondait affirmait qu'il n'y avait personne de ce nom à ce numéro.

> "Le débiteur dit appartement 3 au lieu de F. Le débiteur cherche le numéro de téléphone dans son cellulaire parce qu'il dit avoir un nouveau numéro et ne plus s'en souvenir. Ayant un doute, je demande le lieu de naissance et la date de naissance et le débiteur est valide. Lorsque je transfère le débiteur à l'agent responsable, la ligne coupe. Pensant avoir coupé la communication accidentellement, je rappelle le débiteur. La personne qui répond est alors surprise de voir que je la "rappelle" et on comprend ensemble que c'est le conjoint de Mme P., un certain Christian, qui s'est fait passer pour elle. (Signalement #98)

---

[36] Traduction libre de *call back procedure.*

Dans le signalement qui suit, l'agent a contacté le véritable client et ce dernier lui a confirmé qu'il n'avait pas appelé.

> "Il a prétendu avoir une demande de révision en cours depuis mai 2008 (inexact). Demande quelle adresse nous avons au dossier puisqu'il n'a pas eu de nouvelles de sa demande de révision. Il raccroche lorsque je lui propose d'appeler l'administration puisque je n'ai pas de dossier à son nom. J'ai cru à une rupture involontaire et j'ai rappelé le client. C'est alors que j'ai constaté la tentative frauduleuse. Le client m'a dit que sa fille avait également reçu un appel de la RAMQ le concernant. Il n'a aucune idée de qui ça peut être et pourquoi on le rechercherait. La même tentative aurait été faite pour obtenir des renseignements au centre d'appel, à l'unité administrative N et O". (Signalement #91)

Les initiatives des employés de rappeler des clients ont permis de constater que les fraudeurs n'hésitent pas à mentir concernant leurs coordonnées. Pour l'organisme public, la procédure de rappeler les clients ciblés par des appels suspects est difficilement envisageable pour des raisons de productivité, car cela soulèverait plusieurs questions préoccupantes pour la clientèle.

3.5.2. Les signes subjectifs

Parmi les signes subjectifs les plus fréquents, nous avons noté les erreurs dans l'adresse, le numéro de téléphone ou le montant de la prestation. Cependant, comme l'ont souligné les agents, ces erreurs doivent être interprétées avec réserve, car il arrive fréquemment que les informations au dossier ne soient pas mises à jour. Ainsi, une erreur dans ces éléments ne fait pas en sorte que l'appel est considéré systématiquement comme suspect. Par contre, dans certains contextes, des erreurs dans l'adresse peuvent être considérées comme des signes pertinents de fraude. Comme nous l'avons mentionné, les fraudeurs prétendent souvent déménager fréquemment. Si l'agent voit dans le dossier que la personne n'a pas déménagé récemment ou que le fraudeur est incapable de donner l'une de ses anciennes adresses, l'agent pourra facilement identifier la fraude.

Lors du protocole, il arrive également que le client hésite à une question, car il doit chercher l'information. Si l'hésitation se répète à plusieurs questions, l'agent considérera l'appel comme suspect. Certains agents considèrent aussi comme un signe suspect que la personne n'a pas l'information avec elle au moment de l'appel, car un message électronique lors de l'attente spécifie au client d'avoir les documents avec eux pour accélérer le processus. Il arrive également

que la personne refuse de divulguer de l'information, car elle dit que c'est confidentiel. Cette situation arrive fréquemment avec le NAS et le numéro de compte de banque et il est impossible pour l'agent de savoir si la personne a l'information avec elle ou s'il ne s'agit que d'un prétexte.

Quant aux habiletés développées, plusieurs agents ont mentionné avoir acquis au fil des années une très bonne ouïe. Cette habileté est particulièrement utile et pertinente dans deux types de situation. Tout d'abord, les agents sont capables de reconnaître rapidement la différence entre la voix d'une personne de 20 ans et de 40 ans. Lorsqu'une personne appelle pour une dame de 40 ans, les agents sont capables de savoir si le timbre de la voix correspond à la catégorie d'âge. S'ils ont des doutes, l'agent portera davantage attention aux réponses de la personne.

Ensuite, ils ont développé une sensibilité aux bruits ambiants. Ainsi, les agents peuvent identifier certains sons qui ne sont pas cohérents avec la situation de l'interlocuteur. Par exemple, des sons de voiture alors que la personne dit être chez un ami ou le son de nombreux téléphones qui sonnent alors qu'il prétend être seul chez eux. Cette habileté demande de porter une attention particulière à tous les éléments de chaque appel ce qui demande un effort considérable et beaucoup d'expérience. Dans la citation suivante, l'agent décrit comment il interprète les bruits ambiants :

> "Les bruits ambiants, des fois, ils sont déjà à l'unité administrative et ils sont déjà en file d'attente pour parler à l'agent. Le bruit ambiant, ça se peut que ce soit normal. Mais moi, je le demande, où êtes-vous présentement?". (Entretien #7)

Enfin, les agents sont capables d'identifier facilement les demandes d'information qui sont irrégulières. Comme nous l'avons mentionné, les tentatives non autorisées d'obtention de renseignements personnels sont des événements atypiques, si bien que les agents sont en mesure de reconnaître les demandes qui sortent de l'ordinaire. La majorité des appels se déroulant normalement, lorsqu'une personne désire absolument connaître l'adresse au dossier, le montant d'allocation ou le solde de sa dette, l'agent peut considérer cet appel comme suspect.

Bien que ces éléments contribuent d'une manière plus ou moins égale à l'identification de tentatives non autorisées d'obtention de renseignements personnels, c'est l'accumulation de plusieurs signes subjectifs qui fait en sorte que l'accès est refusé. Cependant, pour l'agent,

l’absence de critères fixes rend l’identification des tentatives difficiles car il ne peut pas seulement se baser sur un élément précis pour refuser l’accès. De plus, les agents ont une certaine réticence face à la détection des tentatives. Comme le mentionne l’agente C, leur mission n’est pas d’effectuer des enquêtes sur chaque personne qui appelle, mais bien d’offrir un service à la clientèle. Pour citer l’agente :

> "Dans le fond, c'est vrai que nous, notre travail, on n'est pas des agents de conformité, notre travail, c'est de donner un service à la clientèle. Si la personne réussit à donner les bonnes informations pour faire le protocole, nous après ça, on continue normalement". (Entretien #8)

Nous pouvons retenir de cette section que, outre certains indices concrets, la plupart des signes permettant aux agents d’identifier les appels suspects contiennent une partie importante d’interprétation. En fait, les signalements sont principalement basés sur l’intuition individuelle en plus des éléments concrets, ce qui fait en sorte que chaque agent trace sa propre ligne de ce qu’il considère comme une fraude. Suivant ce constat, il serait pertinent pour les organisations de développer une formation qui permet d’améliorer la vigilance des agents.

3.6. Refuser l’accès

Lorsque l’agent juge qu’il y a trop de signes qui laissent croire que la personne n’est pas celle qu’elle prétend être, il refuse l’accès. Lorsque cette situation se produit, tous les agents s’en tiennent aux consignes émises par l’organisme public et disent à la personne qu’il n’y a pas de dossier qui correspond aux informations transmises. Par la suite, il lui demande de se présenter dans une unité administrative avec deux pièces d’identité et une personne mettra à jour son dossier et répondra à ses questions. Il est très important lorsque l’agent refuse l’accès de ne pas mentionner l’item qui ne fonctionne pas dans le protocole d’identification et aussi de ne pas dire si la personne est cliente de l’organisation ou non, car ce simple renseignement est en soit confidentiel. Si une tierce personne désire avoir accès au dossier, l’agent lui mentionne qu’il est soumis à la loi sur la protection des renseignements personnels et qu’en raison de cette loi, ils ne peuvent pas donner de l’information à moins qu’une procuration ne soit signée. Une procuration est un document signé, une fois par année, par le client de l’organisation autorisant un tiers à effectuer des modifications dans le dossier du client.

Quant aux réactions du client, elles sont relativement variées. Évidemment, plusieurs haussent le ton et sont frustrés de ne pas avoir de réponse à leurs questions. D'autres menacent de porter plainte contre l'agent, lui dit qu'il fait mal son travail alors que d'autres vont même jusqu'à insulter l'agent. Cependant, contrairement à ce que l'on pourrait croire, un nombre considérable de signalements ne se termine pas dans l'agressivité, mais plutôt dans une certaine coopération. L'agent réussit à faire comprendre à la personne qu'il ne peut confirmer son identité et qu'il ne donnera aucune information. Il est possible de croire que plusieurs présumés fraudeurs préfèrent ne pas attirer l'attention en étant agressif, car rien ne les empêche de raccrocher et d'appeler une nouvelle fois.

3.7. Le signalement

Si les agents ont une grande liberté dans ce qu'ils considèrent comme de la fraude, nous avons remarqué qu'ils ont aussi une liberté lorsque vient le temps de signaler à l'organisation une tentative non autorisée d'obtention de renseignements personnels. Encore une fois, bien qu'il s'agisse d'une obligation pour les agents de signaler toute tentative non autorisée d'obtention, il arrive que pour diverses raisons ils préfèrent ne rien signaler. Il peut s'agir d'un manque de volonté ou d'un manque de temps. De plus, certains agents peuvent être peu enclins à rapporter les situations où des renseignements personnels sont communiqués à un tiers par peur d'être accusés de mal faire leur travail.

Il est impossible de vérifier quel est le pourcentage des tentatives illégales qui sont effectivement signalées. Bien que certaines tentatives d'obtention de renseignements personnels soient flagrantes, la majorité d'entre elles sont davantage le résultat de situations ambiguës qui laissent beaucoup de place à l'interprétation. En l'absence de balises claires sur les cas de présumés fraudeurs, chaque agent définit à sa manière les situations qui sont des tentatives illégales et celles qui ne méritent pas d'être signalées. Pour citer un agent, selon lui, seules les situations les plus évidentes sont signalées.

3.8. Les motivations des présumés fraudeurs

Maintenant que la séquence d'interaction a bien été décrite, il nous semble approprié de tirer des conclusions générales concernant les motivations des fraudeurs. Dans notre analyse, nous avons principalement insisté sur les tentatives qui ont été détectées par les agents et qui n'ont pas résulté

d’une communication non autorisée de renseignements personnels. Nous avons volontairement mis l’accent sur cette catégorie, car elle est représentative de l’ensemble des signalements. En analysant les signalements dans leur ensemble, il nous est possible d’identifier les renseignements recherchés par les fraudeurs et ainsi en déduire les principales motivations. En fait, cette déduction nous permet de répondre à la question suivante : Lorsqu’un fraudeur communique avec l’organisme public, quelles informations cherche-t-il à obtenir? Le tableau 4 présente les renseignements que tentait d’obtenir le présumé fraudeur. Selon les statistiques, l’adresse du client (46,8 %) est l’information la plus recherchée. Ainsi, l’une des motivations les plus fréquentes serait de retrouver une personne.

Tableau 4 Types de renseignements recherchés par le présumé fraudeur

	(n) 1136*	%
Adresse du client	532	46,8
Autres renseignements	263	23,2
Allocation envoyée	201	17,7
Aucune requête (client quitte avant)	91	8,0
Solde de la dette	68	6,0
Montant de l’allocation	66	5,8
Numéro d'assurance maladie	31	2,7
Présence à l'aide	29	2,6
Numéro d'assurance sociale	30	2,6

*Le (n) est plus élevé que le nombre de signalements, car il est possible que des agents aient coché plusieurs éléments pour la même tentative.

Lors d’un entretien avec une agente, cette dernière nous a relaté une situation qu’elle a vécue où le fraudeur avait réussi à obtenir l’adresse du client:

> "Moi ça m'est arrivé une fois. Une femme très pressée, elle avait déménagé et son adresse ce n'était pas clair, bref elle m'a donné son NAM et les autres éléments du protocole. Je réponds à ses questions et elle revient en me demandant c'est quoi l'adresse au dossier, je ne lui réponds pas, elle pose d'autres questions. Elle me redemande l'adresse, je lui dis c'est elle que vous m'avez donné, le 10 de la rue F. Bien non, elle ne me l'avait pas donnée. Pis paf, elle raccroche. J'étais insulté. Je (le signalement) l'ai fait tout de suite après, mais je m'étais fait avoir". (Entretien #10)

En observant les résultats du tableau 4, il est également intéressant de noter que 91 cas, soit 8 % des signalements, la personne a quitté la ligne probablement parce qu'elle ne pouvait pas répondre à une question du protocole. Autre élément intéressant, lors des 61 cas (5,3 %), le fraudeur tentait d'obtenir des renseignements très confidentiels soit le numéro d'assurance sociale ou le numéro d'assurance maladie. Le solde de la dette, qui correspond à 68 cas (6 %), est également un renseignement hautement confidentiel pour l'organisme public. Voici un exemple de signalement où le fraudeur a réussi à obtenir le montant de la dette :

> "Monsieur donne NAS. Il confirme l'adresse et ce qui m'a paru louche c'est qu'ensuite il m'a demandé si c'est ce que j'avais au dossier et il me donne un numéro de téléphone, car on n'avait pas son téléphone au dossier. Monsieur demande le solde de la dette donc je lui donne : je lui demande comment il compte rembourser la dette. Il m'offre un montant. Je lui en propose un autre. Monsieur dit ok et il raccroche. Je rappelle au numéro qu'il m'a donné et la dame qui répond me dit qu'elle ne connaît pas le client". (Signalement #130)

Par contre, contrairement au NAS, le solde de la dette n'est pas une demande irrégulière ce qui fait en sorte que le nombre de tentatives pourrait être beaucoup plus élevé et il est, par conséquent, difficile à associer à une tentative d'obtention non autorisée. Dans le même ordre d'idées, il est impossible de savoir dans ces statistiques combien de fraudeurs ont réussi à savoir si la personne est client de l'organisme public, car cette information s'obtient de différentes manières qui sont difficilement détectables. En ce qui concerne les 263 cas catégorisés sous *Autres renseignements*, l'agent n'a pas pu identifier ce que la personne tentait d'obtenir. Il est possible que la personne n'ait pas réussi le protocole ou que l'agent n'ait pas complété cette section de la fiche.

L'analyse des signalements nous a également permis d'identifier que certains fraudeurs utilisent une technique appelée *breading*. L'objectif du *breading* est d'aller chercher une information en particulier afin de rendre plus crédible une demande ultérieure. L'information recherchée peut être le nom d'une personne, élément technique ou un numéro de téléphone. Ces éléments peuvent sembler anodins et sans valeur, mais lorsque le fraudeur a tous ces renseignements, sa demande est beaucoup plus crédible. Évidemment, ces situations sont très ambiguës et difficiles à détecter. Le signalement qui suit illustre un cas de *breading*:

> "Monsieur désire avoir des nouvelles à la suite de sa nouvelle demande. Lorsque je commence à l'informer, il me demande son numéro civique. Je lui donne. Il me dit qu'il n'a pas d'appartement et avant il en avait un. Je lui dis que c'est correct et il me demande son numéro de téléphone. Je l'informe que l'adresse et son numéro de téléphone sont conformes. Il met fin à l'appel. J'ai vérifié (dans une base de données de l'organisation), il y avait 3 notes de 3 agents différents qui avaient eu ce client avec échec au protocole. J'avais déjà eu ce client environ vers les 14 h 30. Je n'avais pas été en mesure de faire le protocole. Il ne donnait pas la bonne adresse et il ne connaissait pas l'ancienne adresse. Il me demandait quelle ancienne adresse vous voulez". (Signalement #158)

L'analyse des renseignements recherchés par le fraudeur nous permet de conclure que l'une des motivations principales des tentatives non autorisées d'obtention des renseignements personnels est de retrouver le lieu de résidence d'une personne. Cette conclusion concorde avec les travaux de Hart (2010), que des individus, souvent des investigateurs privés ou des journalistes, sont à la recherche de l'adresse de la personne ou de son numéro de téléphone. Ainsi, les organisations publiques possédant une banque importante d'information sur l'ensemble de la population seraient des cibles intéressantes pour des voleurs professionnels.

Donc, cette section nous a permis de dresser un portait détaillé du phénomène de tentatives non autorisées d'obtention de renseignements personnels pour une organisation publique. Afin de bien illustrer les particularités de l'acte frauduleux, nous avons utilisé le concept de script. Cette méthode d'analyse nous a permis de diviser en séquence le phénomène pour en faire ressortir les particularités et ainsi élaborer une description claire des stratégies employées par la grande majorité des fraudeurs. Toutefois, la séquence présentée n'explique qu'une partie des éléments structurants l'opportunité de vol de renseignements personnels pour cette organisation. Lors de la prochaine section, nous identifierons et analyserons les éléments présents dans l'organisation qui influencent l'interaction entre le présumé fraudeur et l'agent du centre d'appel.

4. Les éléments influençant l'opportunité d'obtention de renseignements personnels

Nous allons donc consacrer cette section à l'analyse des éléments organisationnels et individuels qui structurent l'opportunité des tentatives de vol de renseignements personnels. Notre démarche d'analyse s'inscrit dans l'approche situationnelle développée par Cornish (1994). Cette approche permet de mettre en place des mesures qui visent à prévenir, contraindre et arrêter une activité criminelle en manipulant l'environnement afin d'augmenter les efforts du criminel et les

possibilités de détection (Clarke, 1992). Les techniques de prévention du crime développées par Clarke (1980; 1995) & Cornish (1994) sont particulièrement populaires depuis les années 1990, car elles proposent un ensemble de techniques accessibles pouvant avoir un impact relatif sur la criminalité.

Cependant, en plus de son pragmatisme anglo-saxon qui peut parfois sembler simpliste (Cornish, 1994, p. 153), on peut reprocher aux auteurs de la prévention situationnelle d'accorder très peu d'importance aux contraintes inhérentes des environnements et des comportements individuels. Ainsi, les auteurs laissent croire qu'il est possible d'appliquer parfaitement le modèle théorique de la prévention du crime à une situation concrète. Toutefois, dans la réalité, l'application de la prévention situationnelle se heurte à d'importantes contraintes sociales ou organisationnelles qui limitent son efficacité.

Donc, l'objectif de cette section est d'identifier les différentes logiques organisationnelles et humaines présentes dans l'organisation qui influencent l'interaction entre le fraudeur et l'agent. Cette analyse nous permettra de comprendre comment l'opportunité de vol de renseignements personnels est structurée dans un contexte plus large et quelles sont les interrelations entre les facteurs. De plus, en intégrant ces éléments dans notre démarche d'analyse, nous serons davantage en mesure de proposer des solutions adaptées aux contraintes de l'organisation. Dans un premier temps, nous présenterons comment l'expérience de l'agent et sa perception du phénomène influencent la gestion du phénomène. Par la suite, nous discuterons des éléments organisationnels qui influencent l'obtention de renseignements personnels.

4.1. La formation de l'agent et sa perception du phénomène

Selon nos analyses, nous croyons que deux éléments individuels influencent l'opportunité de vol de renseignements personnels. Tout d'abord, il semblerait que l'expérience professionnelle de l'agent a un impact important sur la manière dont ils gèreront les tentatives. Ensuite, le second facteur est la perception que les agents ont du phénomène.

À la lumière des entrevues effectuées avec les agents, nous pouvons distinguer deux catégories d'agents dans le centre d'appel de l'organisme public, soit un groupe au bagage sociologique et

un autre au bagage administratif. Les deux groupes se différencient par leur expérience et leur conception du travail. Les agents du premier groupe pourraient être identifiés comme ceux ayant une formation en sociologie, car ils ont souvent une formation en sociologie, psychologie ou d'anciens travailleurs sociaux. Les agents de ce groupe travaillent dans l'organisation pour offrir un service à des personnes dans le besoin et ils apprécient la relation d'aide qui s'établit avec le client. Nous avons remarqué dans le discours de ces agents, qu'ils ont tendance à faire confiance plus rapidement au client que ceux qui sont en administration. En matière de fraude, pour un agent « prosocial », le client est la bonne personne tant que celui-ci ne prouve pas le contraire.

Le deuxième groupe d'agent serait celui « proconformité ». Ces derniers portent une plus grande attention aux procédures et à l'assurance qualité. Ils sont davantage rejoints par les problèmes de sécurité et ils vont appliquer le protocole d'identification plus rigoureusement. Ce sont probablement eux qui vont signaler le plus de tentatives non autorisées. À l'inverse de l'agent social, pour un agent « proconformité », le client au téléphone n'est pas la bonne personne tant qu'il ne le prouve pas. En raison de cette conception, ces agents ont probablement moins de chance de se faire manipuler par des fraudeurs. Un agent décrit la formation du personnel du centre d'appel comme suit :

> "Je te dirais qu'ici il y en a à peu près la moitié qui ont un côté social avec un DEC ou un certificat en psychologie ou des choses comme ça. L'autre côté vient plus du côté administratif puis c'est correct, il faut s'ajuster. «…» notre job arrive entre les deux. C'est une mixte 50 / 50. On doit être 50 % social, 50 % administratif dans le traitement de la job". (Agent #7)

Ensuite, il nous apparaît pertinent d'analyser la manière dont les agents conçoivent le phénomène, car les perceptions influencent la manière dont ils agiront dans certaines situations. Cette perception est inévitablement modulée par la formation, la personnalité et l'expérience de l'agent. En premier lieu, nous avons remarqué que les tentatives non autorisées d'obtention de renseignements personnels sont un phénomène rare dont les motivations et les conséquences sont très abstraites pour les agents. En ce qui concerne la fréquence, les agents disent qu'il s'agit de situation très rare voire inexistante. En effet, ce constat est confirmé par les statistiques que nous avons présentées. Cependant, si la perception des agents quant à la fréquence est juste, ils sont convaincus que le nombre total d'événements est minime. En fait, lorsque nous leur mentionnions le nombre total de signalements depuis quatre ans, ils étaient tous surpris de

l’ampleur du phénomène. On remarque donc qu’il y a une divergence entre l’ampleur réelle du phénomène et la perception des agents.

Par contre, il semble que c’est davantage les conséquences abstraites qui influencent la perception des agents. Ces derniers ne comprennent pas pourquoi une personne chercherait de l’information dans l’organisme public. Il semble que le fait de ne pas saisir les motivations des fraudeurs fait en sorte que les agents ressentent moins l’obligation de s’impliquer dans les signalements. Selon les agents, l’absence de conséquences directes pour l’organisation, voire même pour le client, fait en sorte qu’il ne s’agit pas d’un problème qui mérite une attention accrue. Les propos recueillis lors de l’entrevue #9 résument bien la pensée de certains : «*Il n’y a rien à aller chercher, on s’entend que ce n’est pas une carte de crédit avec 100 000 $ dessus*». Ainsi, il est raisonnable de croire que la rareté du phénomène et l’absence perçue de conséquence influencent non seulement la perception des agents, mais également la manière dont les mécanismes de protection sont appliqués.

Lorsque nous avons questionné les agents sur ce qu’ils définissaient comme une tentative, ces derniers ont soulevé une distinction intéressante entre les échecs au protocole et les tentatives. En fait, pour les agents, une personne qui échoue le protocole d’identification, pour diverses raisons, n’est pas nécessairement une tentative non autorisée à moins que cette dernière cherche à obtenir des renseignements sur le dossier. Pour être considérée comme une tentative non autorisée, la personne au téléphone doit insister pour obtenir des informations au dossier. Dans ces conditions, chaque agent fait une distinction entre les deux, ce qui laisse beaucoup de place à l’interprétation. Certes, les deux concepts se chevauchent, mais cela ne signifie pas la même chose. Cet extrait d’un entretien avec un agent explique clairement la différence entre les deux concepts :

> "Une tentative non autorisée et un échec au protocole pour moi, c'est vraiment différent et la plupart, c'est des échecs au protocole. Mais une tentative, c'est comme une fois, tu entends des téléphones ou la personne te dis ok je vais te donner cette information là debord. Des fois, la personne qui fait les tentatives n'est pas subtile, des fois, elle l'est beaucoup. C’est mon instinct peut-être, j'analyse trop des fois. Je ne veux pas faire perdre le temps aux gens qui analysent ça aussi. Si j'ai plus que 50 % de doute que c'est une tentative, je vais faire une fiche (de signalement). Mais la plupart du temps, il y a beaucoup d'échecs au protocole […] Quand on commence ici, on a de la misère à faire le dosage entre ce qui est une tentative et ce qui est un échec au protocole". (Entretien #7)

Lorsque nous questionnons les agents sur qui pouvait tenter d'obtenir des renseignements personnels, il semble que tous les agents, peu importe leur expérience professionnelle, ont une conception du fraudeur très professionnel. C'est-à-dire que le fraudeur sait comment fonctionne l'organisation et il est préparé. Selon les agents, ils réussissent à détecter les appels de certains fraudeurs inexpérimentés, mais le vrai fraudeur va passer inaperçu. En fait, les agents considèrent que les vraies tentatives sont presque impossibles à détecter. Cela implique donc que les agents croient qu'ils ne peuvent rien faire pour les détecter.

4.2. Les éléments organisationnels structurant l'opportunité de vol de renseignements personnels

En matière de protection de l'information, l'une des principales vulnérabilités que nous avons identifiées est l'incompatibilité entre trois logiques organisationnelles. Jusqu'ici, la littérature sur la sociologie des centres d'appel nous a permis de saisir l'importance de la productivité et de la qualité du service à la clientèle. Bien qu'il soit possible d'établir un équilibre entre ces deux objectifs, ils sont difficilement conciliables. À la suite de nos analyses, nous croyons que le concept de sécurité est le troisième élément qui influence l'opportunité d'obtention de renseignements personnels. Selon nous, l'opposition entre les objectifs de productivité, de qualité du service à la clientèle et de sécurité, au sein de l'organisation représente des failles exploitables par les délinquants. Ainsi, nous analyserons comment ces éléments interagissent entre eux et comment ils influencent l'opportunité d'obtention de renseignements personnels.

4.2.1. La productivité : L'importance des statistiques

La revue de la littérature nous avait déjà indiqué que la productivité était l'un des éléments les plus présents dans le quotidien des centres d'appel. Les entretiens réalisés avec les agents nous ont permis de confirmer que l'atteinte des statistiques est en effet très importante. Dans un centre d'appel, la productivité se mesure principalement par le calcul du nombre d'appels traités et du temps nécessaire pour répondre au besoin du client. La grande majorité des agents s'entendent pour dire que la productivité est inhérente à tous les centres d'appel. Comme le dit un agent lorsque nous discutions de l'importance des statistiques : « c'est un centre d'appel quand même». Comme nous l'avons mentionné, l'application de la principale mesure de sécurité, le protocole d'identification, occupe une place importante à chaque appel ce qui entre en conflit direct avec la

productivité. Les propos qui suivent résument bien l'opposition entre la productivité et la sécurité :

> "Quand ça l'a été long de faire ton protocole parce que la personne attend un peu, je vais aller chercher ça, là, tu attends. Après ça, c'est un stress parce que tu le sais que ça fait 3-4 minutes. Pis ensuite, les appels c'est censé être 4 minutes fak déjà les 4 minutes sont dépassées et tu ne sais même pas ce qu'elle veut. Là tu dis, j'espère qu'elle sait ce qu'elle veut. Veut, veut pas, on n'est pas sans y penser. Ça fait partie de notre vie, les statistiques. Dans les centre d'appel, c'est sur le nombre d'appels pas sur la qualité". (Entretien #8)

Ces propos rejoignent les écrits sur les centres d'appel qui soulignent que l'importance des statistiques est beaucoup plus importante dans un centre d'appel que dans n'importe quel autre environnement de travail. Ce constat est quelque peu surprenant dans la mesure où nous aurions pu nous attendre à des résultats différents en raison des améliorations des conditions de travail et qu'il s'agisse d'un emploi gouvernemental. Cependant, ces éléments, bien que positifs ne modifient pas la nature même du travail qui est de répondre à de nombreux appels de courte durée.

Les agents savent que les objectifs organisationnels et les attentes de l'employeur sont faits en fonction des statistiques. Dans l'organisation, la cible est de passer quatre minutes ou moins en ligne avec chaque client. Selon les agents, cette cible a un impact sur leur travail. Ainsi, les employés tentent de prendre le moins de temps possible lors de chaque appel afin d'atteindre un maximum de productivité. Lors de l'entretien #2, l'agente nous a décrit l'impact des statistiques sur le travail d'un agent dans un centre d'appel :

> "Le premier stress, c'est la productivité et ça c'est relié aux attentes de l'employeur. Quand tu ne rencontres pas tes stats, tu te fais rencontrer. Ça se retrouve dans ton rapport d'évaluation à la fin de l'année et dans ton évaluation de rendement". (Entretien # 2)

De plus, lors d'une rencontre réunissant tous les agents du centre d'appel en 2009, les agents ont répondu à un questionnaire afin d'améliorer l'efficacité du centre d'appel. Une forte majorité a répondu que l'atteinte des objectifs des statistiques était la chose la plus importante dans leur travail. Cet élément est particulièrement intéressant, car il signifie que les agents accordent de manière générale une place prépondérante aux nombres d'appels traités par jour. Ils ont intégré les objectifs de rendement comme une valeur personnelle symbolique de leur compétence et de

leur efficacité. Ainsi, on peut affirmer que le cercle d'influence de la productivité sur les autres objectifs organisationnels est très important.

En matière de protection de l'information, ce constat est d'une très grande importance. La productivité est à la fois une valeur intégrée par les agents et une source de pression importante qui inévitablement va influencer la manière dont le protocole d'identification est appliqué. Selon les agents, il revient à chacun de gérer cette pression. Selon un agent, certains négligeraient l'aspect de sécurité afin de mieux gérer cette pression :

> "Moi je pense que quand on vit une pression au niveau des statistiques, oui on va escamoter ça (le protocole). Parce que tu veux éliminer. Par exemple, tu vis un stress au travail, tu veux l'éliminer". (Entretien #2)
>
> […]
>
> "Mais je suis sûre qu'il (protocole d'identification) y en a qui l'escamote pour tout plein de raison, pour des raisons de statistiques, pour des raisons de productivité, mais d'un autre côté ça peut mettre en danger, le côté sécurité qui a été tassé". (Entretien #2)

Bref, afin de réduire la pression inhérente à la productivité constante, les agents peuvent appliquer le protocole le plus simplement possible pour accélérer le traitement des appels. Cette stratégie facilite le travail de l'agent, mais aussi celui du client. L'agent peut également décider de ne pas remplir la fiche de signalement, car ceci allonge son temps post-appel. En effet, des statistiques sont également compilées sur le temps passé *hors-ligne*. Les agents doivent donc tenter de limiter le temps post-appel pour diminuer cette statistique et répondre à un plus grand nombre d'appels. Lorsque l'agent décide de compléter une fiche de signalement à la suite d'une tentative, il doit prendre au moins 5 minutes et demeurer hors ligne. Donc, nous retrouvons une double pénalité dont la première consiste en l'allongement de l'appel dû à une application rigoureuse du protocole et la seconde dans le temps additionnel perdu à compléter la fiche de signalement. Ainsi, il est important de réaliser que le programme de détection de tentatives non autorisées d'obtention de renseignements personnels est basé sur un incitatif négatif.

4.2.2. Qualité du service à la clientèle : Diversité des appels et type de client

La qualité du service à la clientèle est également un objectif organisationnel important. Pour les agents, un service à la clientèle de qualité signifie qu'il a été en mesure de répondre adéquatement aux questions du client. Comme nous l'avons souligné dans notre revue de la littérature, cet objectif est difficilement conciliable avec celui de la productivité. Cette réalité est

particulièrement vraie pour les agents des centres d'appel, car ils doivent à la fois répondre adéquatement aux demandes du client et maximiser le nombre d'appels par jour. Les agents doivent alors trouver un équilibre difficile entre la quantité et la qualité. Ceci fait en sorte que les agents travaillent dans un contexte ambivalent où chaque appel fait l'objet d'un dilemme entre ces deux objectifs.

De plus, les agents de l'organisation travaillent dans un contexte particulier qui les place dans un contexte encore plus ambivalent. En effet, ils doivent répondre à une très grande variété de demandes. La diversité des appels est certainement un des éléments qui complexifie le travail des agents. Les propos de l'agent illustrent bien la diversité des appels à gérer.

> "Une fois, une fille voulait se suicider. Là, moi après ça fallait que je prenne un autre appel. Des fois, il faut lâcher ça et aller prendre une marche. Mais ça c'est une partie de mon travail, après ça je vais avoir une vieille dame qui veut un formulaire de lunettes. Un autre qui fait un échec au protocole. Un autre qui est crampé parce qu'il vient de se trouver une job qui veut annuler son dossier pis après ça, on va dîner. Faut être capable de mettre la switch à off. Les signalements, le protocole, c'est des parties importantes de notre travail, mais il y a des choses bien plus graves au téléphone. J'ai une femme de Fermont qui m'a appelé en cachette en disant mon mari va arriver, pis, il va me donner une volée, aidez-moi. Là, moi faut que je gère ça. Pis là, tu prends un autre appel et un gars qui s'est trouvé une job. Les tentatives c'est important, mais faut se mettre en contexte". (Entretien #7)

Si les demandes sont diversifiées, la clientèle l'est tout autant. En effet, tous les agents rencontrés ont mentionné que la clientèle de l'organisme public était particulière et qu'il était essentiel d'en prendre conscience, car cela influence inévitablement leur travail. Les agents de l'organisme public offrent un service de dernier recours à des gens dans le besoin. Plusieurs ont des déficiences légères, des problèmes de santé mentale et ils ont peu d'interaction sociale. Une agente tient des propos quelque peu surprenants sur la clientèle de l'organisation :

> "Disons que tu prends une caisse populaire, dans la journée d'une caissière, combien de clients démunis va-t-elle avoir? Aucun. Dans un commerce, tu vois 10 % - 20 % de démunis, ce n'est pas quelque chose d'exceptionnel, mais qui n'est pas dans la moyenne. Nous autres, notre moyenne, c'est du monde bizarre". (Entretien #1)

La diversité des appels et la clientèle particulière de l'organisation font en sorte que le travail des agents est très exigeant psychologiquement et émotionnellement. Ces deux éléments sont des facteurs additionnels qui s'ajoutent à la pression inhérente à la productivité et à la qualité du service à offrir que nous avons déjà abordé. Dans ce contexte, il est raisonnable de croire que les agents sont dans une position vulnérable et que la prise de décision dans ce contexte est complexe. Bien que nous n'ayons pas de preuve concrète, nous croyons que les fraudeurs sont avantagés dans leur tentative par ces éléments. De plus, nous avons remarqué qu'avec la notion de service à la clientèle vient la notion de bon service. Les agents souhaitent être en mesure de répondre adéquatement à la demande du client et de l'aider. Les fraudeurs sont conscients que l'agent doit répondre à leur demande et ils appuient leur scénario sur la notion de bon service à la clientèle pour obtenir des renseignements confidentiels.

4.2.3. La sécurité : L'application du protocole

Nous proposons d'introduire un troisième élément aux contraintes organisationnelles, la sécurité. Bien que la sécurité soit un élément secondaire pour plusieurs organisations, on remarque que les mesures de sécurité en matière de protection de l'information occupent une place de plus en plus importante dans les organisations. Les données collectées lors de nos entretiens nous suggèrent que les mesures de sécurité en place dans l'organisme sont des éléments qui influencent l'opportunité de vol de renseignements personnels. Quant à notre terrain de recherche, on remarque qu'une partie importante des appels est allouée à l'application du protocole d'identification. Cependant, l'application de mesure de sécurité telle que le protocole d'identification a un impact considérable sur les objectifs de productivité et de service à la clientèle.

Pour les agents, le protocole fait partie intégrante de leur travail. Il est intéressant de remarquer que quatre agents nous ont mentionné que l'objectif du protocole va bien au-delà de seulement poser des questions :

> "Parce que, dans le fond c'est aussi pour les protéger eux que je fais ça, ce n'est pas simplement pour moi". (Entretien #4)

Ainsi, les agents sont conscients que la raison d'être du protocole est double. Il permet à la fois de protéger les renseignements personnels et de protéger le client. De plus, dans la mesure où la

clientèle de l'organisme public est défavorisée et plus à risque de conflit, cet élément n'est pas à négliger. Un agent utilise une métaphore intéressante pour décrire l'utilité du protocole :

> "C'est comme une porte, si on veut que les gens entrent plus vite pour les servir plus vite, on a juste à donner la clé à tout le monde ou à la laisser ouverte. Par contre, au niveau de la sécurité, ça serait trop flagrant. Donc, il faut choisir à qui on la donne la clé puis comment ils font pour entrer". (Entretien #7)

Il est également surprenant de constater que les agents considèrent que le protocole est profitable dans une certaine mesure au service à la clientèle. Contrairement à certains agents qui trouvent que le protocole nuit à la relation avec le client, selon plusieurs, le protocole permet d'établir le contact avec le client. Voici comment une agente considère le protocole :

> "Ça prend environ 90 à 105 secondes (pour faire le protocole). Moi, si on enlève le protocole, je vais parler avec le client pendant 5 secondes. Je vais me sentir comme une machine. Le protocole débute une interaction avec le client, c'est le début de la conversation. Moi, je regarde le dossier, nom et adresse et les autres éléments inscrits". (Entretien #1)
>
> […]
>
> "Moi, je trouve qu'en questionnant, ça permet d'établir un contact. Comment la personne se sent-elle? Moi, ça permet de me positionner sur mon attitude à avoir. Calme si la personne est nerveuse. Sans ça, c'est oui, non, ok, bye. Le but n'est pas d'étirer le protocole, mais. Parce qu'il y a des personnes qui appellent, mais que l'on ne connaît pas les motivations. Elles peuvent appeler quelques minutes plus tard pour obtenir d'autres informations. J'essaie de faire une auto-évaluation personnelle pour savoir si mon protocole est assez complet". (Entretien #1)

Une autre utilité au protocole est qu'il permet de poser des questions sur l'état du dossier. Plusieurs agents ont mentionné que s'ils se contentaient de poser les trois mêmes questions lors du protocole d'identification, il n'y aurait jamais de problème. Par contre, lorsque l'agent varie ses questions ou qu'il en pose davantage, il a plus de chance de trouver des erreurs ou des anomalies dans le dossier. De plus, il est indéniable que c'est lorsque l'agent pose plus de questions qu'il détecte les tentatives non autorisées. Évidemment, pour des raisons de productivité et de service à la clientèle, mais également parce que cela est exigeant mentalement, il est impossible pour les agents d'adopter cette pratique à tous les appels. De plus, il semble clair que pour les agents du centre d'appel, il est impossible d'être alerte à 100% à tous les appels. Ils

doivent donc décider des appels qui méritent de poser davantage de questions. Une agente rencontrée nous explique l'interaction entre les facteurs organisationnels et comment un agent vit avec les pressions inhérentes de ce travail :

> "Ce n'est pas facile. La personne ne pense plus aux statistiques ou tu viens d'avoir un appel assez difficile et long. Quand on dit que l'on doit être alerte à chaque appel, c'est du stock. T'as fini de parler pendant 6 à 8 minutes avec quelqu'un qui ne comprend pas parce même toi t'as eu de la misère à comprendre la loi. T'essaies de lui mettre dans un langage qu'il peut comprendre, ce n'est pas simple. Toi, ton prochain appel, t'as le goût que ce soit simple et que ça aille bien. Et ça se peut que ça aille bien, mais c'est ça qui a glissé. Ce n'est pas de ta faute. C'est tous ces facteurs-là, c'est à ce moment qu'on réalise combien c'est délicat ce travail d'interprétation et d'interaction avec des personnes. C'est exigeant, mentalement et psychologiquement et physiquement parce que tu dois rester assis. En plus, il y a tout ça. Faut avoir effacé tout ce qu'il y a avant et dire que l'on repart". (Entretien #3).

Ainsi, nous remarquons qu'il y a différentes visions du protocole. Si tout le monde s'entend pour dire que le protocole d'identification est nécessaire, les agents ne l'appliquent pas tous à la même intensité. Certains vont se contenter de faire le minimum et ils vont peut-être même fermer les yeux sur certaines situations alors que d'autres agents vont être beaucoup plus vigilants. Parlant de ses collègues, une agente mentionne :

> "Ma voisine peut très bien dire, moi il me demande 3 éléments, pis il rentre (dans le dossier) et je m'en fou". (Entretien #4)

Il est également intéressant de remarquer qu'il est facile pour certains agents de refuser l'accès alors que pour d'autres, il s'agit d'un irritant important. Pour plusieurs agents, l'application du protocole est un irritant non seulement parce qu'il nuit à leur statistique, mais aussi parce qu'il nuit à la qualité du service à la clientèle. La clientèle signifie parfois leur mécontentement face aux nombreuses questions et à la longueur du protocole. Il ne fait aucun doute que le protocole d'identification est répétitif. De plus, il arrive fréquemment que l'application du protocole soit plus longue que la demande du client. Ainsi, certains agents le considèrent comme un obstacle important et ils préfèreraient qu'il soit aboli ou automatique. Selon certains agents, le protocole d'identification est aussi un irritant pour le client.

> "Sauf que là, on vient…c'est un irritant pour eux autres, mais c'est un irritant pour nous aussi. Ça commence mal la conversation quand il dise bon….il commence avec un ton". (Entretien #6)

Nous avons donc démontré qu'il y a une grande diversité des points de vue quant à la raison d'être du protocole. En analysant la manière dont le protocole d'identification est perçu, nous pouvons déduire la manière dont la sécurité est perçue et appliquée dans l'organisation. Il est important de saisir comment la principale mesure de sécurité est perçue, car cela nous permet d'apporter les correctifs nécessaires au niveau de son application.

Enfin, ce chapitre nous a permis de saisir d'une part, l'ampleur de ce phénomène pour l'organisation et d'autre part, les interactions qui s'établissent entre le fraudeur et l'agent. En utilisant un schéma illustrant le déroulement de tentatives, nous avons été en mesure de dégager les particularités des tactiques mises en place par les fraudeurs. Par ailleurs, en dernière partie de ce chapitre, nous avons analysé l'influence de facteurs organisationnels et individuels sur l'opportunité d'obtention de renseignements personnels. Ainsi, les demandes organisationnelles contradictoires, la manipulation émotive des fraudeurs, le stress de l'environnement sont tous des éléments qui empêchent l'agent de prendre une décision optimale.

CHAPITRE IV :

DISCUSSION ET CONCLUSION

Tout au long de cette recherche, nous avons exploré le phénomène de tentatives non autorisées d'obtention de renseignements personnels pour un organisme public. Afin d'atteindre notre objectif général qui consistait à décrire et à analyser le phénomène, nous avons rencontré dix-neuf (19) agents d'un centre d'appel et nous avons examiné 1 136 signalements. Alors que plusieurs organisations pourraient croire qu'une personne qui tente d'obtenir des renseignements personnels sur un individu est un incident isolé, les résultats de notre recherche viennent mettre en lumière un phénomène bien plus présent que l'on pourrait croire. Par notre approche empirique unique, nous en sommes parvenus à identifier les caractéristiques globales du phénomène ainsi que les tactiques utilisées par les fraudeurs.

Afin de mieux comprendre les tentatives non autorisées d'obtention de renseignements personnels, nous nous sommes inspirés du cadre de l'analyse stratégique afin d'élaborer une méthode d'analyse hybride qui permet à la fois de décrire les tactiques utilisées par le délinquant et le rôle de l'environnement dans le déroulement du délit. Conséquemment, notre analyse s'est déroulée à deux niveaux. Dans un premier temps, cette stratégie nous a permis d'identifier, à l'aide du concept de script, une séquence d'interaction entre les agents et les fraudeurs applicables à la majorité des tentatives documentées par l'organisme public. Ainsi, nous avons été en mesure de dégager neuf étapes qui rythment les échanges entre les deux principaux acteurs. Cela nous a permis d'identifier les tactiques utilisées par les fraudeurs ainsi que les mécanismes de détections développés par ceux-ci. Cependant, s'il ne fait aucun doute que l'interaction entre le fraudeur et l'agent est l'élément central des tentatives, nous considérons qu'il est indispensable d'analyser le phénomène au-delà de l'interaction binaire entre les protagonistes afin de mettre en place des stratégies efficaces de prévention du crime. C'est pour cette raison que nous avons choisi d'analyser les contraintes présentes dans l'environnement, mais également les leviers disponibles afin de rendre l'activité frauduleuse plus difficile.

Notre objectif principal de recherche consistait à dresser un portrait détaillé des stratagèmes utilisés par les fraudeurs lors de communication téléphonique. Parmi les éléments les plus intéressants, notons que la principale motivation des fraudeurs qui communiquent avec le l'organisme public est de retrouver une personne. Trois éléments nous permettent d'avancer cette conclusion. Tout d'abord, les agents mentionnaient, dans 46,8% des signalements, que le fraudeur tentait d'obtenir des informations sur l'adresse du client. Ensuite, les fraudeurs utilisent

souvent le prétexte du changement d'adresse qui n'a pas fonctionné ou du document non reçu pour essayer d'obtenir la véritable adresse du client. Par la suite, la richesse des informations contenues dans le cas Martine nous révèle que certaines personnes peuvent mettre beaucoup d'effort pour retrouver une personne. Ce constat permet de réaliser qu'il est faux de croire que l'adresse d'une personne est un renseignement banal et sans valeur. Il est donc important pour les organisations de sensibiliser leur personnel à l'importance de protéger non seulement les renseignements sensibles tels que le NAS et le NAM, mais également les informations concernant l'adresse de la clientèle.

De plus, notre terrain de recherche démontre empiriquement que l'utilisation du *pretexting* est très fréquente et qu'il s'agit d'un problème qui menace l'intégrité des renseignements personnels détenus par une organisation. Le *pretexting* consiste à prétendre être une autre personne afin de tromper et d'obtenir des informations confidentielles. Les statistiques de l'organisation témoignent que les fraudeurs affirme effectivement être le client ou un employé de l'organisation afin d'obtenir de l'information. Si, dans notre étude, il semble plus efficace de prétendre être un employé, il est raisonnable de croire que ce ne sont pas tous les fraudeurs qui sont en mesure de réunir les éléments essentiels : langage, information et attitude, pour y arriver. Ainsi, la majorité des cas signalés dans l'organisme public implique des personnes qui allèguent être le client. Enfin, nous avons constaté que les fraudeurs n'hésitent pas à donner de fausses informations pour rendre leur scénario crédible.

Parmi les caractéristiques des appels frauduleux les plus intéressants, nous avons remarqué que la confiance occupe un rôle central dans le succès ou l'échec d'une tentative. Les fraudeurs disposent de peu d'outils pour créer un lien avec l'agent et ainsi augmenter leur chance de succès. Par contre, dans le contexte d'appel téléphonique très court, le fraudeur a seulement besoin de créer un lien de confiance suffisant pour manipuler l'agent. Une fois le lien créé avec l'agent, le fraudeur abuse de la confiance de ce dernier pour obtenir l'information. Ainsi, il semble que le fait d'être aimable et d'utiliser un langage approprié au contexte sont deux éléments essentiels à la réussite d'une tentative. Les fraudeurs utilisent aussi fréquemment l'appel à l'autorité en prétendant être un policier ou un avocat. Bien que les agents avouent que cela influence leur comportement dans la mesure où ils sont quelque peu déstabilisés, nous avons remarqué que l'utilisation de ces personnages aurait l'effet contraire. Par exemple, lorsqu'une personne prétend

être un avocat, cela sème presque automatiquement un doute dans la tête de l'agent et il sera plus attentif au protocole.

Pour répondre à notre premier sous-objectif, nous avons analysé les statistiques compilées par l'organisation au cours des quatre dernières années. Ainsi, nous avons remarqué une croissance constante et marquée du nombre de signalements. Selon nous, cette tendance pourrait être due à deux facteurs. Elle serait attribuable à la fois à une augmentation réelle du nombre de tentatives non autorisées d'obtention de renseignements personnels et à une amélioration significative de la capacité de détection des agents des centres d'appel. S'il nous est difficile d'évaluer l'impact réel de ces deux explications, il semble évident que si une organisation forme ses employés adéquatement à détecter les appels suspects et qu'elle développe des outils adaptés à leur environnement, ils en identifieront davantage. C'est dans ce contexte que l'organisme public a été en mesure d'identifier 1 136 tentatives non autorisées d'obtention de renseignements personnels en quatre ans. Ainsi, contrairement à ce que l'on pourrait croire la détection de tentatives non autorisées est davantage associée à une excellente sécurité qu'à des défaillances. Ce nombre élevé de tentatives détectées démontre empiriquement qu'il y a une réelle menace à la sécurité des renseignements personnels et que contrairement à ce que plusieurs organisations seraient portées à croire, ces tentatives ne sont pas des incidents isolés. De plus, il est raisonnable de croire que les organisations publiques sont des cibles privilégiées des fraudeurs en raison de la quantité d'information qu'elles détiennent et de l'environnement de travail. Selon nous, il est possible que si toutes les organisations publiques mettaient en place un système de détection et de collecte d'information sur les tentatives non autorisées d'obtention de renseignements personnels, ils obtiendraient des résultats semblables à notre milieu de recherche.

Enfin, les données disponibles sur l'ampleur du phénomène nous amènent à nous demander si les tentatives non autorisées d'obtention sont un problème sous-évalué ou surévalué. Certes, il semble clair que plusieurs situations frauduleuses ne sont pas signalées par les agents. Comme nous l'avons mentionné, différents facteurs individuels et organisationnels peuvent faire en sorte qu'un agent signale une tentative ou non. En raison de l'importance de ce chiffre noir, nous devons interpréter avec précaution les statistiques. S'il est difficile de nier la présence d'un chiffre noir, il faut également prendre en considération les faux positifs, c'est-à-dire les demandes légitimes qui sont considérées comme des tentatives non autorisées. En effet, il est possible que

des appels non frauduleux aient été considérés comme des tentatives non autorisées ce qui gonflerait artificiellement le nombre de tentatives.

Ensuite, afin répondre à notre deuxième sous-objectif, nous avons analysé comment les accès frauduleux sont perçus et gérés sur le terrain par les agents des centres d'appel. Tout d'abord, nos entretiens ont révélé que les agents perçoivent les tentatives comme des incidents isolés et sans conséquence. Selon nous, cette perception est due à trois éléments. Premièrement, l'organisation publique ne subit aucune conséquence directe de la divulgation non autorisée de renseignements personnels. Deuxièmement, pour les agents, les motivations des fraudeurs sont abstraites et ils ont de la difficulté à comprendre pourquoi quelqu'un voudrait obtenir l'adresse ou le montant de la dette d'une personne. Troisièmement, les agents n'ont pas conscience du volume total des tentatives signalées. Ces trois éléments modulent la conception que les agents ont du phénomène et influencent leur comportement par rapport aux tentatives. En raison des éléments identifiés, nous croyons que les agents n'adoptent probablement pas le comportement optimal afin de protéger les renseignements personnels, car ils ont une perception altérée. Malgré tout, les agents ont signalé un nombre impressionnant de tentatives ce qui démontre encore une fois la présence du problème. Nos entretiens nous ont également permis de réaliser que les agents ont une perception très idéaliste du fraudeur. En d'autres termes, les agents croient que les fraudeurs sont très professionnels et extrêmement efficaces à un tel point qu'il leur est impossible de les détecter. Cette conception est accompagnée d'un sentiment d'impuissance qui nous laisse penser que les agents préfèrent croire qu'il n'est pas possible pour eux de détecter les fraudeurs.

En ce qui concerne la gestion des appels suspects, nous remarquons que les agents se basent principalement sur des signes subjectifs pour identifier les tentatives non autorisées. Comme nous l'avons souligné, les tentatives sont très variées et la grande majorité est le résultat de situations ambivalentes et en l'absence de repères établis, l'agent se fie davantage à son intuition qu'à des signes objectifs pour identifier une tentative. De plus, cette recherche a permis de mettre à jour la réelle ambiguïté quant à la définition d'une tentative illégale d'obtention de renseignements personnels. Nous avons remarqué que chaque agent élabore sa propre définition, en fonction de son bagage professionnel et de son expérience. Par conséquent, chacun trace sa propre ligne entre ce qui est une tentative et ce qui ne l'est pas. Évidemment, cela a un impact important en matière de sécurité de l'information, car chaque appel fait l'objet d'un niveau différent d'attention. Certes, il est impossible d'atteindre l'harmonie parfaite en raison des différences individuelles,

mais il est tout de même possible de limiter les divergences. Ce constat illustre le besoin pour une organisation de fixer des balises claires afin de limiter les interprétations individuelles. Donc, il est primordial d'effectuer des séances de sensibilisation afin de donner l'heure juste aux employés sur le problème et sur les directives. En donnant régulièrement des informations sur l'ampleur du phénomène et les conséquences potentielles pour l'organisme et la clientèle, l'organisation motivera ses employés et ces derniers seront plus alertes.

La dernière section du troisième chapitre nous a permis de répondre aux deux derniers sous-objectifs soient d'expliquer comment les éléments organisationnels présents dans l'environnement des agents structurent l'opportunité de vol de renseignements personnels et de définir la position organisationnelle des agents et son impact sur la protection des renseignements personnels. Afin d'y arriver, nous avons analysé trois objectifs organisationnels qui ont un effet direct sur la protection des renseignements personnels détenus par l'organisation. Tout d'abord, nous sommes parvenus à la conclusion, à la suite de nos entretiens, que la productivité est une valeur intégrée par tous les agents. Ces derniers sont conscients que l'efficacité de leur travail est directement mesurée par l'atteinte d'objectif quantitatif. Cette évaluation constante exerce une pression significative sur la gestion du temps des appels. Ainsi, pour limiter la pression et améliorer leurs statistiques, des agents pourraient accélérer la réponse aux appels en limitant, entre autres, les questions au protocole d'identification. Afin d'améliorer la protection de l'information, il serait donc pertinent de travailler sur la manière dont cette pression est perçue et gérée par les agents. Si la pression liée à la productivité est inhérente à tous les centres d'appel, l'organisation peut revoir le message qui est transmis aux agents à l'égard des statistiques. De plus, elle peut aider les agents à gérer la pression afin de limiter les impacts non seulement sur la protection de l'information, mais également sur la qualité du service offert.

Ensuite, en analysant le rôle de l'objectif lié au service à la clientèle, nous avons remarqué que la diversité des appels ainsi que la clientèle particulière de l'organisation font en sorte que le travail des agents est exigeant psychologiquement et émotionnellement. Les agents sont déjà dans une position complexe dans la mesure où ils doivent trouver un équilibre difficile entre le temps pour répondre à la demande du client et la qualité de la réponse transmise. Ainsi, en ajoutant une diversité d'appel et une clientèle complexe à gérer, nous sommes convaincus que les agents se trouvent dans une position très ambivalente et qu'il est très difficile pour eux de prendre une

décision optimale en matière de sécurité. Bref, nous pouvons avancer que les employés de cette organisation sont dans une situation encore plus difficile et que des mesures additionnelles doivent être mises en place afin de protéger efficacement les renseignements personnels de la clientèle.

Enfin, nous avons intégré le concept de sécurité aux objectifs organisationnels. Selon nous, cet ajout est le reflet de la nouvelle réalité des organisations qui conservent des renseignements personnels et il nous semblait indispensable d'analyser l'impact de la sécurité de l'information sur la dynamique organisationnelle. Nos rencontres nous ont permis de réaliser que l'application du protocole d'identification est en conflit direct avec les objectifs de productivité. Nous avons également remarqué que les agents le considèrent comme une nécessité qui est cependant appliquée à différentes intensités selon l'agent et la situation. En fait, nous avons identifié différentes visions de la sécurité par l'interprétation du protocole d'identification, ce qui nous laisse croire qu'il n'est pas appliqué de manière uniforme. Il serait donc important pour l'organisation de réafficher clairement son engagement à protéger les renseignements personnels de sa clientèle et d'uniformiser les pratiques de tout son personnel.

Quant à la relation entre le service à la clientèle et la sécurité, il semble que ces objectifs soient davantage conciliables. En effet, certains agents nous ont mentionné que le protocole d'identification leur permet, entre autres, d'établir une conversation avec le client et de savoir dans quel état d'esprit ce dernier se trouve. Pour l'organisation, il serait donc intéressant d'utiliser ce levier pour inciter les agents à appliquer un protocole rigoureux. De plus, l'organisation doit réfléchir sur le message qu'elle transmet à ses employés en ce qui a trait au protocole d'identification, car nos entretiens avec les agents nous ont appris que si ces derniers se contentaient d'appliquer le minimum du protocole d'identification, très peu de tentatives seraient identifiées. La majorité des signalements sont alors le fruit d'initiative de la part des agents qui posent davantage de questions ou qui demandent un numéro de téléphone pour rappeler. L'organisation doit donc décider si elle encourage ces initiatives au détriment des objectifs de productivité et de service à la clientèle.

D'un point de vue scientifique, cette recherche dresse le portrait détaillé d'un phénomène qui était jusqu'à présent méconnu voire ignoré. Les données empiriques utilisées démontrent que les tentatives non autorisées d'obtention de renseignements personnels ne sont pas des incidents

isolés et il est fort probable que le secteur public soit une cible particulièrement intéressante en raison de la quantité impressionnante d'informations personnelles qu'il conserve. Dans une certaine mesure, cette recherche a démontré qu'il est nécessaire d'élargir notre compréhension des menaces existantes à la protection de l'information. Dans notre milieu de recherche, le fraudeur n'était jamais en contact physique avec les renseignements personnels et il n'avait même pas à se déplacer ou à effectuer une copie numérique de l'information pour les obtenir. Cependant, le résultat est le même, des renseignements personnels ont été communiqués à une tierce personne sans l'autorisation du client.

De plus, cette recherche a permis de réaliser toute la complexité pour une organisation de protéger les renseignements personnels qu'elle possède. Une protection complexe qui doit, selon nous, s'articuler autour de l'élément humain. Depuis plusieurs années, des efforts considérables ont été faits d'un point de vue technologique afin de protéger les renseignements personnels. Certes, l'informatique fait partie intégrante du système de sécurité, mais notre recherche illustre l'importance du facteur humain. D'un côté, nous avons démontré que les délinquants utilisent souvent des moyens rudimentaires et accessibles pour arriver à obtenir des renseignements personnels. De l'autre côté, nous avons insisté sur l'importance de comprendre comment les principaux acteurs en matière de protection de l'information, ici les agents des centres d'appel, perçoivent le phénomène et leur rôle dans l'organisation. Une fois que l'on comprend leur point de vue, il est possible de mettre en place des leviers afin d'influencer leurs comportements de manière à minimiser les risques de communication non autorisés de renseignements personnels.

Notre recherche a également souligné l'importance de comprendre l'environnement dans lequel évolue un phénomène criminel afin de mettre en place des solutions efficaces. Selon nous, il est aussi important de comprendre les contraintes de l'environnement que l'événement lui-même. Dans trop de recherche, l'attention est seulement mise sur l'analyse du phénomène au détriment de l'environnement. Or, il nous apparaissait essentiel de présenter le phénomène d'obtention de renseignements personnels, non pas seulement en terme de *modus operandi* mais comme intimement lié à son environnement. Les personnes qui tentent d'obtenir illégalement des renseignements personnels profitent des contraintes entre les objectifs de productivité, de qualité service à la clientèle et de sécurité pour arriver à leur fin. En analysant comment ces éléments interagissent, il nous est possible de les utiliser comme levier afin de mettre en place des mesures de protection efficaces.

Ce travail de recherche nous amène à nous demander si le cadre légal présentement en place permet une protection réellement efficace des renseignements personnels. Loin de nous la prétention de faire une analyse exhaustive de l'efficacité de la Loi sur la protection des renseignements personnels (LPRP), mais il nous semble pertinent d'aborder la question de la sécurité des renseignements personnels détenus par le gouvernement. Tout d'abord, selon nos observations, les mesures de protection, présentement en place dans l'organisation, permettent de protéger efficacement les renseignements personnels de la clientèle. Cependant, il ne fait aucun doute que la loi élaborée il y a plus de 25 ans, période durant laquelle se sont produits des changements capitaux dans l'automatisation de l'information et des données électroniques, et dans le déploiement d'Internet et du Web, ne soit pas adapté aux complexités de la gouvernance contemporaine (Flaherty, 2008, p. 11). Bien qu'il ne soit pas inhabituel qu'un texte de loi ne soit pas modifié rapidement, le cas de la LPRP est particulièrement inquiétant si l'on tient compte des menaces réelles à la sécurité de données et les conséquences pour la vie privée. Le commissaire à la protection de la vie privée, principal acteur fédéral, a signifié à plusieurs reprises au législateur le besoin d'examiner en profondeur et de réformer cette loi afin de l'adapter au contexte actuel. Cependant, la réforme d'un texte de loi de premier plan comme la LPRP est très complexe et demande beaucoup de volonté politique.

Certes, les problèmes de la situation législative actuelle sont multiples, mais en ce qui concerne les renseignements détenus par les organisations publiques, nous en avons retenu trois. Tout d'abord, selon David B. Flaherty, professeur émérite de l'Université de Western Ontario et premier commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique (2008, p. 17), les contrôles sont trop indulgents dans le secteur public. En fait, il est assez surprenant de réaliser que les contrôles sont moins sévères dans le secteur public que dans le secteur privé. Il ne fait aucun doute que le commissariat à la protection de la vie privée effectue un travail colossal, mais il n'a pas les ressources et les outils pour attaquer le problème de front[37]. Les vérifications sont fastidieuses et au bout du compte, les institutions gouvernementales ne sont pas tenues d'appliquer les recommandations du commissariat. Comme l'explique la commissaire, Mme Jennifer Stoddart, il est essentiel qu'un organisme indépendant soit en mesure d'effectuer

[37] Témoignage de Jennifer Stoddart devant le Comité de l'accès à l'information, des renseignements personnels et de l'éthique de la Chambre des communes, 8 avril 2008. http://www.priv.gc.ca/information/pub/pa_ref_add_080417_f.cfm

des contrôles sérieux des pratiques de gestion de l'information lorsqu'il s'agit d'éléments aussi importants que des renseignements personnels :

> "La Loi sur la protection des renseignements personnels est la pierre angulaire des relations informationnelles entre les organismes gouvernementaux et les personnes. Si le cadre législatif régissant ces relations est chancelant, c'est tout l'édifice de la responsabilité qui est menacé. La protection des renseignements personnels est trop importante pour être soumise aux caprices de la politique et de la gestion internes."

Ensuite, le deuxième problème que nous avons identifié est que peu de politiciens se soucient de la protection des renseignements personnels, sauf lorsqu'une crise survient. En effet, lorsque des situations embarrassantes se produisent, les établissements perdent beaucoup de temps à rétablir la situation, mais outre ces situations très couvertes médiatiquement, la protection des renseignements personnels dans les organisations publiques est un sujet impopulaire. Selon M. Flaherty (2008, p. 4) bien que les sondages démontrent une grande inquiétude à l'égard de la préservation de la vie privée, le manque de leadership et d'engagement politique a nuit au progrès jusqu'à ce jour[38]. En fait, la réforme de LPRP n'est pas un sujet qui capte l'attention du gouvernement, des politiciens ou des bureaucrates. Cependant, la pression populaire est peut-être l'un des seuls moyens pour que les choses changent.

Enfin, l'absence d'obligation légale de notification de pertes de renseignements personnels donne une très grande liberté aux organisations. Certes, les organismes sont encouragés à développer des lignes directrices relatives à la notification, mais rares sont ceux qui le font et ceux qui sauront quoi dire aux clients inquiets (Flaherty, 2008, p. 42). Il serait essentiel dans la future législation d'inclure des exigences légales pour la gestion des atteintes à la vie privée en informant, par exemple, le commissariat et le client. De plus, si des renseignements personnels sont perdus ou communiqués en raison de la négligence d'une personne ou de l'organisation, des sanctions devraient être appliquées. Cependant, l'approche du législateur devrait être de mettre en place des incitatifs légaux ou économiques afin d'augmenter la conformité et la transparence des organisations.

---

38 Voir le sondage Ekos mené en 2006 au nom du Commissariat à la protection de la vie privée du Canada à : http://www.privcom.gc.ca/information/survey/2006/ekos_2006_f.asp.

Dans le cadre de notre recherche, l'organisation en question n'avait pas mis en place un système clair de notification avec les clients dont des renseignements personnels avaient été communiqués. Bien qu'il soit évident que ce type de mesure peut avoir d'importantes répercussions pour l'organisation, nous croyons qu'il serait préférable qu'elle informe le client. Après tout, l'organisation a rempli toutes les exigences en matière de sécurité et il serait surprenant que la communication non autorisée soit le résultat d'une négligence. De plus, selon la commission d'accès à l'information du Québec, lorsqu'une perte de renseignements personnels se produit, l'organisme doit prendre les moyens nécessaires afin d'éviter ou de limiter le préjudice que les personnes concernées peuvent subir. Informer rapidement les personnes concernées est un moyen efficace de limiter ou même de prévenir tout préjudice. Pour l'organisation, il s'agirait d'une preuve de transparence importante qui serait en quelque sorte la continuité du programme en place.

D'un point de vue pratique, cette étude est un exemple concret de l'importance de documenter les événements liés à la sécurité des renseignements personnels, de cumuler de l'information et des connaissances sur un problème afin de mettre un système de protection efficace. Selon Vermeij (2008), en collectant ainsi de l'information, on améliore la force et la longévité d'un système de sécurité, car la menace devient plus clair et prévisible. Il est ainsi plus facile de s'adapter à la menace. Cependant, une telle stratégie nécessite la mise en place de mécanismes de collecte et de traitement de l'information (Vermeij, 2008, p. 32). En plus, l'organisme doit utiliser les connaissances développées pour améliorer le système en place. Pour ces raisons, l'organisation dans laquelle la recherche a eu lieu est en quelque sorte un modèle, car elle ne s'est pas contentée d'appliquer le protocole d'identification, mais bien de mettre en place un processus de signalement, de développer des outils, de former les agents et d'ajuster les mécanismes de protection à la suite des analyses. Leur système de protection est caractérisé par une adaptation à la menace qui est possible grâce à une collecte et une analyse de l'information collectée par les agents. Enfin, l'analyse de l'information recueillie permet également d'identifier les éléments que l'on ne connait pas sur la menace. Connaissant les informations manquantes, il est possible de mettre en place des mesures spécifiques pour les obtenir.

Afin d'améliorer le système en place dans l'organisation, cette recherche a été accompagnée d'un rapport de recommandation. Pour les besoins du mémoire, nous avons retenu les

recommandations les plus pertinentes pour le plus grand nombre d'organisations possibles. Les recommandations présentées sont le fruit de l'expérience vécue dans l'organisation, de l'analyse de données recueillies et de discussions informelles avec du personnel de l'organisation. Ainsi, nous avons réuni les recommandations en quatre grands axes que nous avons nommés : mobilisation, sensibilisation, formation et intervention. Chaque groupe de solutions est complémentaire aux autres dans la mesure où aucune n'assure une protection totale, mais que chaque partie est essentielle pour obtenir une protection efficace.

La première étape est de nommer une personne responsable de la protection des renseignements personnels. Cette personne aurait pour mission de coordonner les actions à prendre en matière de protection de l'information entre la direction, le département des technologies et les employés. Pour les organisations de plus grande envergure, il serait pertinent de créer un comité ou une table de consultation avec plusieurs intervenants impliqués dans la manipulation de renseignements personnels. La personne responsable aurait pour rôle de créer et de coordonner des initiatives en matière de protection de l'information, d'aller chercher les ressources pertinentes qu'elles soient à l'interne ou à l'externe, d'identifier les besoins et de prendre des mesures nécessaires. Une leçon que nous pouvons tirer de l'organisation dans laquelle a eu lieu la recherche est qu'il est essentiel de libérer au moins une ressource compétente qui serait en mesure de faire preuve de leadership dans ce dossier. Par la suite, cette personne doit développer des outils afin de permettre la collecte d'information sur les incidents qui impliquent directement ou indirectement la communication ou la perte de renseignements personnels. Ces informations doivent être compilées dans une base de données pour devenir la mémoire de l'organisation en matière de sécurité.

Une fois les outils développés, il est essentiel de mobiliser les employés de première ligne en les informant et en les formant sur les principes de la protection des renseignements personnels[39]. Il est pertinent de créer un canal de communication direct entre les employés de première ligne et le responsable de la protection des renseignements personnels. Ainsi, ils pourront communiquer directement avec le responsable de manière régulière et ainsi transmettre leurs commentaires sur ce qui se déroule sur le terrain.

[39] Les sites Internet du Commissariat à la protection de la vie privée et La commission d'accès à l'information du Québec offrent des lignes de conduite sur les principes de la Loi sur la protection des renseignements personnels.

Le deuxième axe est la sensibilisation des employés. Tout d'abord, l'organisation doit réfléchir sérieusement au message qu'elle transmet en matière de productivité, de service à la clientèle et de sécurité. Comme nous l'avons présenté, si une organisation insiste seulement sur les objectifs de productivité, il sera extrêmement difficile de développer des habitudes de travail sécuritaire. La manière dont les employés perçoivent la sécurité est fortement influencée par le message et le comportement de l'organisation (Kraemer et al., 2009, p. 517). L'organisation doit donc s'assurer de transmettre le message que la sécurité est l'une des priorités.

Par la suite, les employés doivent être informés sur les enjeux légaux de l'organisation en matière de protection des renseignements personnels et des conséquences potentielles de la communication non autorisée de renseignements personnels. Lors des périodes d'information, il serait pertinent de souligner l'importance de leur travail dans le cadre de la protection des renseignements personnels. De plus, selon nos analyses, il est essentiel de bien informer les employés sur la nature et la forme concrète du problème afin de les motiver. Différents thèmes tels que les impacts de la communication non autorisée de renseignements personnels sur la clientèle, les conséquences sur la réputation de l'organisation et les conséquences du vol d'identité pourraient être abordées lors de ces périodes de sensibilisation. Cette sensibilisation a pour objectif de mieux informer les employés et de susciter une participation active de leur part. La sensibilisation peut prendre différentes formes. Évidemment, la plus connue est la session d'information en groupe. Par contre, il serait important de varier les médias de communication afin de mieux informer les agents pour ainsi susciter leur intérêt et maintenir un niveau d'attention relativement élevé.

Le troisième axe est la formation. L'un des résultats intéressants de ce mémoire est qu'il est important pour une organisation, comme un centre d'appel, de travailler sur la manière dont les agents gèrent le stress de leur travail et de leur environnement. Nous croyons qu'en travaillant indirectement sur la gestion du stress liée aux appels et à la productivité, il est possible d'améliorer la protection des renseignements personnels.

Les formations pourraient également être axées sur la gestion des appels suspects. En utilisant des cas concrets, ce type de formation est particulièrement pertinent, car les tentatives non autorisées d'obtention de renseignements personnels sont des événements rares dont la forme demeure

ambiguë pour les employés. En développant une formation spécifique sur la détection des appels suspects et les actions à prendre dans ces situations, l'organisation fournit à ses employés les outils nécessaires afin qu'ils identifient les situations problématiques et qu'ils réagissent efficacement. Cette formation de base qui devrait être reprise annuellement et elle pourrait être jumelée avec la présentation de cas concrets préparés par écrit ou en version audio. Évidemment, la formation par enregistrement audio est beaucoup plus dynamique et appréciée des employés. L'objectif secondaire de ce type de formation est de susciter l'intérêt et d'amener les employés à discuter et à réfléchir sur cet enjeu.

Lors de cette formation, il faudrait faire comprendre aux agents que lors d'un appel, c'est l'accumulation de signes qui justifie le refus de divulguer de l'information et non la présence d'un signe en particulier. Lorsque l'agent perçoit un signe anormal (erreur, manque d'information, pression, sons ambiants, motifs de l'appel, demande de la personne, prétextes), il devrait porter plus d'attention à cet appel et aller plus loin dans le protocole. En prévention de la fraude, il s'agit du principe des indicateurs (*red flag*). Lorsque l'agent remarque la présence de plusieurs indicateurs de fraude, deux actions peuvent être prises : aller plus loin dans le protocole d'identification ou refuser d'accéder au dossier. Par exemple, un client qui met de la pression ne doit pas être considéré automatiquement comme de la fraude, mais il s'agit d'un indicateur. Si ce même client commet une erreur dans des éléments de base du protocole et qu'il hésite sur des questions personnelles alors aucun renseignement ne doit être communiqué et l'agent doit compléter une fiche de signalement.

Le quatrième axe est celui de l'intervention, c'est-à-dire prendre des mesures directes afin de rétablir une situation. À un niveau micro, nous jugeons que l'implantation de directives concernant une procédure de rappel serait particulièrement efficace. Rappelons que la procédure de rappel consiste à communiquer avec le client en utilisant les informations au dossier afin de confirmer que ce dernier est bien entré en contact avec l'organisation quelques minutes auparavant. En effet, notre terrain de recherche nous permet d'avancer qu'il est l'un des moyens les plus efficaces pour s'assurer de l'identité du client. Par contre, cette procédure ne peut pas être utilisée systématiquement, car elle peut avoir des impacts importants sur la productivité et l'image de l'organisation dans la mesure où elle met à jour des failles potentielles au client.

Dans un cadre plus large, nous considérons qu'il est essentiel pour une organisation d'envergure de structurer un processus d'intervention en cas de fraude téléphonique de masse[40], aussi connu sous le nom de *vishing*[41], ou toute autre situation d'urgence impliquant la perte d'une quantité importante de renseignements personnels. La clé pour gérer efficacement les situations d'urgence est la planification. Nous recommandons de mettre en place un processus en deux temps, soit une étape de veille et une étape d'alerte afin d'utiliser plus efficacement les ressources. La veille consiste en une diffusion restreinte de l'information à certains acteurs clés à l'interne, mais elle ne nécessite aucune mobilisation supplémentaire. En d'autres mots, la situation est problématique, mais sous contrôle. Cependant, une attention particulière y est accordée et une enquête plus approfondie ou des mesures additionnelles peuvent être prises si cela est possible. Par exemple, lors de tentatives d'accès répétées à un dossier, un courriel est immédiatement envoyé à tous les employés. Un autre exemple qui peut nécessiter une veille serait un agent qui signale qu'une personne se présentant comme un gestionnaire de l'organisation tente d'avoir des informations sur un client.

Quant à l'alerte, elle consiste à lancer le processus d'intervention afin de neutraliser ou de limiter les préjudices et les dommages pouvant résulter de la perte ou du vol de renseignements personnels. Contrairement à la veille, l'alerte implique une diffusion de l'information beaucoup plus grande et une mobilisation du personnel plus importante. Les situations nécessitant une alerte peuvent aussi bien être une seule communication non autorisée de renseignements personnels, le questionnement des médias sur la perte de renseignements ou une situation de fraude de masse. Selon la loi, l'organisme qui perd ou se fait voler des renseignements personnels doit prendre les moyens nécessaires afin d'éviter ou de limiter le préjudice que les personnes concernées par les renseignements personnels peuvent subir.

---

40 Le 22 juillet 2010, deux attaques vishing ont eu lieu simultanément dans les états de l'Utah, le Wyoming et l'Idaho. Un serveur composait automatiquement des centaines de numéros de téléphone et un message préenregistré prétendant provenir d'une banque locale informait la personne que sa carte de débit avait été désactivée. Les clients étaient invités à composer un numéro sans frais pour avoir de l'information. Une fois le numéro de téléphone composé, le message en attente demandait de composer le numéro de carte et le NIP afin d'accélérer le processus de réactivation. Consulté le 22 juillet 2010 à http://www.bankinfosecurity.com/articles.php?art_id=2771

41 Le vishing est la contraction de VoIP et de phishing. Il s'agit de messages frauduleux envoyés automatiquement à l'aide d'un serveur à un grand nombre de personnes par téléphone. Dans ce mode d'attaque, la cible est invitée à composer un numéro de téléphone et à y communiquer des renseignements sensibles.

En cas d'alerte, les intervenants importants, qui sont préalablement identifiés, doivent être informés de la situation et se rencontrer. Par exemple, le groupe doit réunir les principaux directeurs, les ressources humaines, le responsable de la protection des renseignements personnels, une personne de la direction des communications (gestion des médias), un conseiller juridique, un responsable de la sécurité numérique, etc. Par la suite, une équipe spécifique constituée de quelques personnes doit être désignée pour prendre une décision concernant les actions qui seront prises. L'alerte impliquerait d'informer rapidement la ou les personnes concernées par l'incident, car il s'agit d'un moyen efficace de limiter ou même de prévenir tout préjudice (www. www.cai.gouv.qc.ca). Enfin, lorsque la situation est clairement définie à l'interne, l'organisation peut décider d'informer les autorités extérieures appropriées telles que le service de police (si les circonstances laissent croire à la possibilité d'un crime) et la commission d'accès à l'information.

Bien que notre recherche ait permis de dresser un portrait détaillé du phénomène de tentatives non autorisées d'obtention de renseignements personnels, elle comporte certaines limites qu'il importe de souligner. Tout d'abord, il est évident que les informations exploitées dans cette étude ne constituent que cinquante pour cent (50%) de l'interaction entre les protagonistes. Ainsi, nous avons été en mesure de dresser un portrait du phénomène selon la perspective de l'organisation victime. Ils nous étaient impossibles d'avoir accès aux caractéristiques des personnes qui tentent d'obtenir des renseignements personnels détenus par les organisations. Il s'agit ici d'une piste intéressante, bien que très difficile à exploiter en raison du faible taux d'arrestation, qui permettrait de mieux comprendre les motivations et le point de vue des fraudeurs. De futures recherches pourraient tenter de rencontrer ces personnes et il est probable, au même titre que les travaux de Copes & Vieraitis (2007; 2009; 2008) sur les personnes inculpées de vol d'identité, que les résultats permettraient de démentir une série de préjugés véhiculés dans les médias sur le profil et les activités de ces personnes.

Une alternative beaucoup plus accessible serait d'avoir accès à des enregistrements audio des conversations entre les agents du centre d'appel. L'une des limites de notre recherche est que nous avons seulement eu accès à la retranscription des événements et aux discours des agents. Les enregistrements audio auraient pu fournir de précieux détails quant au climat de l'interaction

et aux stratégies mises en place par le fraudeur. De plus, il aurait été beaucoup plus facile de décrire comment se déroulent les échanges entre l'agent et le fraudeur.

Enfin, nous pouvons nous questionner à quel point, nos résultats sont transposables à d'autres organisations ou d'autres secteurs d'activités. D'abord, il serait faux de croire que notre milieu de recherche constitue une exception dans le secteur des institutions publiques. Nous croyons qu'il est possible que d'autres institutions publiques fassent face à la même menace. Par contre, notre recherche se limite à un centre d'appel d'un organisme public. Ici, l'élément important est avant tout la présence d'un centre d'appel. Ainsi, selon nous, qu'il s'agisse d'un centre d'appel qui relève d'une organisation publique ou privée, si les mêmes caractéristiques propres au centre d'appel sont présentes, nos observations pourraient être utilisées. Par conséquent, le potentiel de généralisation des résultats est limité à l'environnement des centres d'appel.

En réalisant cette étude exploratoire, nous avons été en mesure de faire la lumière sur l'ampleur et les caractéristiques d'un phénomène peu connu, celui des tentatives non autorisées d'obtention de renseignements personnels pour une organisation publique. Bénéficiant d'un accès privilégié à une banque d'information unique, cette recherche fournit des preuves empiriques non seulement sur l'ampleur du phénomène pour l'organisme mais également sur les techniques utilisées par les fraudeurs à la recherche de renseignements personnels. Nous avons également permis de combler plusieurs faiblesses de l'analyse stratégique en prenant soin d'intégrer les contraintes et les dynamiques organisationnelles pour comprendre l'interaction entre le fraudeur et l'agent au moment des tentatives. Ainsi, notre cadre conceptuel ne s'est pas limité à la description des *modus operandi* des fraudeurs, il a illustré la complexité des interactions entre les éléments individuels et organisationnels qui modulent les tentatives non autorisées d'obtention de renseignements personnels.

En outre, nous pouvons retenir que bien que les tentatives soient des événements atypiques dans le quotidien des agents, elles ne constituent pas des événements isolés. Les nombreuses tentatives réelles présentées dans ce mémoire, l'arrestation d'une femme prétendant être une employée de l'organisme public et 1 355 tentatives ne sont que quelques-unes des données qui permettent de le confirmer. Il nous apparaît évident que si l'organisme public et la police investiraient plus de moyens à ce type de délinquance, les arrestations seraient plus nombreuses. À la suite de cette

recherche, nous savons également que les fraudeurs qui auront du succès seront ceux qui parviendront à établir un lien de confiance suffisant avec l'agent. Pour y arriver, des gestes simples, mais significatifs tels qu'adopter une attitude sympathique, prendre des nouvelles de son interlocuteur et adopter un langage commun, ont un impact important dans le succès d'une tentative. Par contre, il est nécessaire que le fraudeur soit préparé, qu'il connaisse l'organisation ainsi que son fonctionnement et qu'il soit prêt à tenter à plusieurs reprises avant d'obtenir des renseignements personnels. Enfin, nous savons que le stress lié aux objectifs de productivité a un impact sur l'application du protocole d'identification et qu'il s'agit d'un levier essentiel à exploiter pour les organisations afin d'améliorer la protection des renseignements personnels. Quant au législateur, il devra au cours des prochaines années élaborer des incitatifs légaux et économiques afin d'augmenter la conformité et la transparence des organisations en matière de protection des renseignements personnels car les contrôles présentement en place ne sont pas suffisants.

Enfin, cette étude s'inscrit dans une foulée de recherche visant à comprendre les menaces à la protection de l'information et il est évident qu'elle est le symbole d'un élargissement des terrains de recherche en criminologie qui illustre de plus en plus la diversité des problématiques criminelles. Certes, la criminologie n'est pas le seul domaine de recherche pertinent et compétent dans l'amélioration de la protection de l'information, mais elle fournit une base théorique extrêmement adaptée à une compréhension plus efficace de la menace. C'est par une compréhension plus juste des défis liés à la protection des renseignements personnels qu'il sera possible d'améliorer les pratiques en matière de sécurité.

Selon nous, le phénomène de tentatives non autorisées d'obtention de renseignements personnels doit être compris à travers la transformation dans la manière dont les services publics sont offerts à la population. L'utilisation de centres d'appel afin de gérer les demandes de la population, la collecte de plus en plus de renseignements personnels et l'utilisation de banques de données informatiques accessible par tous les employés, ont complexifié les enjeux de la protection des renseignements personnels. À mesure que les renseignements personnels sont déplacés d'un environnement physique unique vers un univers numérique, on assiste à une modification des opportunités criminelles. Aujourd'hui, les délinquants, attirés par le rôle prépondérant que jouent les renseignements personnels dans notre société, profitent des failles techniques et humaines dues à la complexité de la protection de l'information. En fait, il est primordial pour les

organisations et les autorités législatives d'identifier et de comprendre les risques de la communication non autorisée de renseignements personnels. Malheureusement, plusieurs organisations sous-estiment les problèmes de sécurité en les banalisant. D'une certaine manière, cette étude démontre qu'il ne fait aucun doute que le 21^{e} siècle comporte des défis de taille en matière de protection des données personnelles et de la vie privée pour la société de l'information.

BIBLIOGRAPHIE

Aksin, Z., Armony, M., & Mehrotra, V. (2007). The modern call center: A multi-disciplinary perspective on operations management research. *Production and Operations Management, 16*(6), 665-688

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security, 26*(4), 276-289

Alicke, M., & Govorun, O. (2005). The Better-Than-Average Effect. Dans M. D. Alicke, D. A. Dunning & J. I. Krueger (dir.), *The self in social judgment*. New York: Psychology Press.

Armor, D., & Taylor, S. (2002). When predictions fail: The dilemma of unrealistic optimism. Dans D. Gilovich, D. W. Griffin & D. Kahneman (dir.), *Heuristics and biases: The psychology of intuitive judgment* (p. 334-347): Cambridge University Press.

Bain, P., & Taylor, P. (2000). Entrapped by the 'electronic panopticon'? Worker resistance in the call centre. *New Technology, Work and Employment, 15*(1), 2-18

Bain, P., Watson, A., Mulvey, G., Taylor, P., & Gall, G. (2002). Taylorism, targets and the pursuit of quantity and quality by call centre management. *New Technology, Work and Employment, 17*(3), 170-185

Beck, U. (1992). *Risk society: towards a new modernity*. Sage Publications Ltd.

Berg, S. (2008). Preventing Identity Theft Through Information Technology Dans Megan M. McNally & G. R. Newman (dir.), *Perspectives on Identity Theft* (Vol. 23, p. 151-167).

Bertrand, Y. (1991). *Culture organisationnelle*. Presse Université du Québec.

Besnard, D., & Arief, B. (2004). Computer security impaired computer security. *Computers & Security, 23*, 253-264

Brantingham, P., & Brantingham, P. (1993). Environment, routine and situation: toward a pattern theory of crime. *Routine activity and rational choice, 5*(2), 259-294

Buscatto, M. (2002). Les centres d'appels, usines modernes? Les rationalisations paradoxales de la relation téléphonique: Call centers, modern factories? The paradoxical rationalization of telephonic relations. *Sociologie du travail, 44*(1), 99-117

Campenhoudt, L., & Quivy, R. (1995). *Manuel de recherche en sciences sociales*. Paris : Bordas.

Carr, M. (2009). *Social and Human Elements of Information Security: Emerging Trends*.

Cialdini, R. (1987). *Influence: Soyez celui qui persuade. Ne soyez pas celui qu'on manipule*. (Édition originale en anglais[e] éd.). New-York: William Morrow & Co.

Cialdini, R. (1993). *Influence: The psychology of persuasion*. Quill New York.

Clarke, R. (1994). Human identification in information systems: Management challenges and public policy issues. *Information Technology & People, 7*(4), 6-37

Clarke, R. (1995). Situational crime prevention. *Crime and Justice*, 91-150

Clarke, R. (1999). *Hot products: understanding, anticipating and reducing demand for stolen goods*. Home Office.

Clarke, R. V., & Cornish, D. B. (1985). Modeling offenders' decisions: A framework for research and policy. *Crime & Just., 6*, 147

Cohen, L., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American sociological review, 44*(4), 588-608

Copes, H., & Vieraitis, L. (2007). Identity Theft: Assessing Offenders' Strategies and Perceptions of Risk. *NCJRS Report, 219122*

Copes, H., & Vieraitis, L. (2009). Bounded rationality of identity thieves: Using offender-based research to inform policy. *Criminology & Public Policy, 8*(2), 26

Copes, H., & Vieraitis, L. (Dir.). (2008). *Risks, Rewards and Strategies of Stealing Identities* (Vol. 23): Criminal JusticePress.

Cornish, D. (1994). The procedural analysis of offending and its relevance for situational prevention. Dans R. V. Clarke (dir.), *Crime Prevention Studies* (Vol. 3, p. 151-196). Monsey, NY: Criminal Justice Press.

Cornish, D., & Clarke, R. (2002). Analyzing organized crimes. *Rational choice and criminal behavior: Recent research and future challenges*, 41–63

Cornish, D. B., & Clarke, R. V. (1986). *The reasoning criminal: Rational choice perspectives on offending*. Springer-Verlag New York.

Curien, N., & Muet, P.-A., (2004). *La société de l'information*. Paris.

Cusson, M. (1986). L'analyse strategique et quelques developpements recente en criminologie. *Criminologie, 19*, 51–72

Cusson, M. (1989). *Délinquant pourquoi?* Montréal: Hurtubise.

Cusson, M., & Cordeau, G. (1994). Le crime du point de vue de l'analyse stratégique. *Traité de criminologie empirique, 2*, 91-112

Dontamsetti, M., & Narayanan, A. (2009). Impact of the Human Element on Information Security. Dans M. Gupta & R. Sharman (dir.), *Social and Human Elements of Information Security: Emerging Trends and countermeasures* (p. 27-42). London: Premier Reference Source.

Dupont, B. (2010). Les organisations: sentinelles aveugles de la sécurité des données personnelles? . *Sécurité & Stratégie*(3)

Dupont, B., & Gagnon, B. (2009). La sécurité précaire des données personnelles en Amérique du Nord. (Note de recherche no. 1), 16

Dupont, B., & Louis, G. (2009). Les voleurs d'identité. (Note de recherche no. 2), 18

Elaad, E. (2003). Effects of feedback on the overestimated capacity to detect lies and the underestimated ability to tell lies. *Applied Cognitive Psychology, 17*(3), 349-363

Fernie, S., & Metcalf, D. (1998). (Not) Hanging on the Telephone: Payment Systems in the New Sweatshops. *London School of Economics*

Flaherty, D. H. (2008). Réflexions sur la réforme de la Loi sur la protection des renseignements personnels. 47

Foucault, M. (1975). *Surveiller et punir*. Gallimard Paris.

Frangopoulos, D. E. (2007). *Social engineering and the ISO/IEC 17799: 2005 security standard: a study on effectiveness.* (University of South Africa, South Africa).

Freedman, J. L., & Fraser, S. C. (1966). Compliance without pressure: The foot-in-the-door technique. *Journal of personality and social psychology, 4*(2), 195

Frey, D. (1986). Recent research on selective exposure to information. *Advances in experimental social psychology, 19*, 41-80

Gandy Jr, O. H. (1989). The surveillance society: information technology and bureaucratic social control. *Journal of Communication, 39*(3), 61-76

George, J., Marett, K., Crews, J., Cao, J., Lin, M., Biros, D. (2004). *Training to detect deception: An experimental investigation*.

Gill, M., & Hart, J. (1999). Private Security: Enforcing Corporate Security Policy Using Private Investigators. *European Journal on Criminal Policy and Research, 7*(2), 245-261

Gordon, D. (1987). The Electronic Panopticon: A Case Study of the Development of the National Criminal Records System. *Politics and Society, 15*(4)

Gordon, G., Rebovich, D., Choo, K., & Gordon, J. (2007). Identity Fraud Trends and Patterns: Building a data-based foundation for proactive enforcement. *Center for Identity Management and Information Protection, Utica College*

Gordon, G., & Willox Jr, M. (2004). Identity fraud: a critical national and global threat. *Journal of Economic Crime Management, 2*(1), 1-48

Greenwald, A., & Banaji, M. (1995). Implicit social cognition: Attitudes, self-esteem, and stereotypes. *Psychological review, 102*(1), 4

Guéguen, N. (2002). *Psychologie de la manipulation et de la soumission*. Paris: Dunod.

Hadnagy, C. (2010). *Social Engineering: The Art of Human Hacking*. Wiley.

Halperin, R., & Backhouse, J. (2008). A roadmap for research on identity in the information society. *Identity in the information society, 1*(1), 71-87

Hammond, K. (2000). *Judgments under stress*. Oxford University Press, USA.

Hart, J. (2010). Criminal infiltration of financial institutions: a penetration test case study. *Journal of Money Laundering Control, 13*(1), 55-65

Jaccoud, M., & Mayer, R. (1997). L'observation en situation et la recherche qualitative. *La recherche qualitative. Enjeux épistémologiques et méthodologiques*, 211-249

Jamieson, R., Land, L., Sydney, A., Sarre, R., Adelaide, A., Steel, A. (2008, 3-5 Dec). *Defining Identity Crimes*. Communication présenté 19th Australasian Conference on Information Systems, Christchurch.

Jones, G., & Levi, M. (2000). The value of identity and the need for authenticity. *Foresight Crime Prevention Panel Essay*

Kahneman, D., Slovic, P., & Tversky, A. (1982). *Judgment under uncertainty: Heuristics and biases*. Cambridge University Press.

Knapp, K., Marshall, T., Rainer, R., & Ford, F. (2006). Information security: management's effect on culture and policy. *Information Management & Computer Security, 14*(1), 24-36

Knights, D., & McCabe, D. (1998). 'What happens when the phone goes wild?': staff, stress and spaces for escape in a BPR telephone banking work regime. *Journal of Management Studies, 35*(2), 163-194

Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security, 28*(7), 509-520

Kray, L., & Galinsky, A. (2003). The debiasing effect of counterfactual mind-sets: Increasing the search for disconfirmatory information in group decisions. *Organizational Behavior and Human Decision Processes, 91*(1), 69-81

Langenderfer, J., & Shimp, T. A. (2001). Consumer vulnerability to scams, swindles, and fraud: A new theory of visceral influences on persuasion. *Psychology and Marketing, 18*(7), 763-783

Langer, E. J., Blank, A., & Chanowitz, B. (1978). The mindlessness of ostensibly thoughtful action: The role of" placebic" information in interpersonal interaction. *Journal of personality and social psychology, 36*(6), 635

Launay, M., & Benedetto, P. (2004). *Psychologie cognitive*. Hachette supérieur.

Leman-Langlois, S. (2002). The myopic panopticon: The social consequences of policing through the lens. *Policing and society, 13*(1), 43-58

Levine, R. (2003). *The power of persuasion: how we're bought and sold*. New-Jersey: John Wiley and sons.

Commissariat à la protection de la vie privée du Canada, (2006). *Lignes directrices en matière d'identification et d'authentification*. Repéré à www.priv.gc.ca/information/guide/auth_061013_f.cfm

Lyon, D. (1994). *The electronic eye: The rise of surveillance society*. University of Minnesota Press.

Mann, I. (2008). *Hacking the human: social engineering techniques and security countermeasures*. Gower Publishing Ltd.

Marett, K., Biros, D., & Knode, M. (2004). Self-efficacy, training effectiveness, and deception detection: a longitudinal study of lie detection training. *Intelligence and Security Informatics*, 187-200

Martin, B. (2004). Telling lies for a better world. *Social Anarchism, 35*, 27-39

Marx, G. (1988). La société de sécurité maximale. *Déviance et société, 12*(2), 147-166

Marx, G. (Dir.). (2001). *Identity and anonymity: Some conceptual distinctions and issues for research*: Princeton University Press.

Mason, J. (2002). *Qualitative researching*. (2nd Edition[e] éd.). London: Sage Publications Ltd.

Mayhew, P., Clarke, R., Sturman, A., & Hough, J. (1975). Crime as opportunity. *Great Britain Home Office Research Planning Unit United Kingdom*, 43

Milgram, S. (1974). *Obedience to authority: An experimental view*. Taylor & Francis.

Mitnick, K., & Simon, W. (2003). *The art of deception: Controlling the human element of security*. John Wiley & Sons, Inc. New York, NY, USA.

Mitnick, K., & Simon, W. (2009). *The Art of Intrusion: The real stories behind the exploits of hackers, intruders and deceivers*. Wiley.

Moir, I., & Weir, G. (2008). Identity Theft: A Study in Contact Centres. *Communications in Computer and Information Science, 12*, 18-25

Morgan, D. L. (1997). *Focus groups as qualitative research.* (Second[e] éd.). London: Sage Publications.

Newman, G. (2008). Identity Theft and Opportunity. *Crime Prevention Studies, 23*, 9-31

Newman, G., & McNally, M. (2005). Identity theft literature review. *United States Department of Justice: National Institute of Justice*

Nohlberg, M. (2009a). *Securing information assets: understanding, measuring and protecting against social engineering attacks.* (Stockholm University, Stockholm).

Nohlberg, M. (2009b). Why Humans are the Weakest Link. Dans M. Gupta & R. Sharman (dir.), *Social and Human Elements of Information Security: Emerging Trends and countermeasures* (p. 15-26). London: Premier Reference Source.

Norris, C., & Armstrong, G. (1999). *The maximum surveillance society: The rise of CCTV*. Berg Publishers.

Office of fair trading, (2009). *The psychology of scams: Provoking and committing errors of judgement*. University of Exeter School of Psychology.

Pires, A. P. (1997). Échantillonnage et recherche qualitative: essai théorique et méthodologique. Dans J. Poupart, Deslauriers, Glroulx, Laperrière, Mayer & Pires (dir.), *La recherche qualitative. Enjeux épistémologiques et méthodologiques* (p. 113-169). Montréal: Gaëtan Morin.

Poupart, J. (1997). L'entretien de type qualitatif: considérations épistémologiques, théoriques et méthodologiques. Dans J. Poupart, Deslauriers, Glroulx, Laperrière, Mayer & Pires (dir.), *La recherche qualitative: Enjeux épistémologiques et méthodologiques* (p. 173-209). Montréal: Gaëtan Morin.

Poupart, J. (1998). *La recherche qualitative : diversité des champs et des pratiques au Québec*. Montréal: G. Morin.

Pyszczynski, T., Greenberg, J., & Solomon, S. (1997). Why do we need what we need? A terror management perspective on the roots of human social motivation. *Psychological Inquiry, 8*(1), 1-20

Rannenberg, K. (2009). *The future of identity in the information society*. Springer Verlag.

Rosa, E. (Dir.). (2003). *The logical structure of the social amplification of risk framework (SARF): Aleratheoretical foundations and policy implications*: Cambridge Univ Pr.

Sarriegi, J., Santos, J., Torres, J., Imizcoz, D., & Plandolit, A. (2006). Modeling Security Management of Information Systems: Analysis of a Ongoing Practical Case. *línea http://systemdynamics. org/conferences/2006/proceed/papers/SARRI206. pdf*

Saunders, K., & Zucker, B. (1998). Counteracting identity fraud in the information age: The Identity Theft and Assumption Deterrence Act. *Cornell JL and Pub. Pol'y., 8*, 661

Schneier, B. (2000). *Secrets & lies: digital security in a networked world*. John Wiley & Sons, Inc. New York, NY, USA.

Schneier, B. (2008). The psychology of security. 26

Simon, H. A. (1982). Models of bounded rationality. *MIT Press, (2 vols.).*

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8*(1), 31-41

Sjöberg, L. (2000). Factors in risk perception. *Risk analysis, 20*(1), 1-12

Slovic, P. (1975). Choice between equally valued alternatives. *Journal of Experimental Psychology: Human Perception and Performance, 1*(3), 280-287

Slovic, P. (1987). Perception of risk. *Science, 236*(4799), 280

Slovic, P. (2000). *Perception of risk* (Risk, society and policy series[e] éd.)

Slovic, P., Finucane, M., Peters, E., & MacGregor, D. (2004). Risk as analysis and risk as feelings: Some thoughts about affect, reason, risk, and rationality. *Risk analysis, 24*(2), 311-322

Slovic, P., Fischhoff, B., & Lichtenstein, S. (1980). Facts and fears: Understanding perceived risk. *Societal risk assessment: How safe is safe enough*, 181-216

Sproule, S., & Archer, N. (2006). Defining Identity Theft–A Discussion Paper. *McMaster eBusiness Research Centre (MeRC), McMaster University*

Stanton, J., Stam, K., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security, 24*(2), 124-133

Synovate, (2007). *Federal Trade Commission: 2006 identity theft survey report*.

Taylor, J., Lips, M., & Organ, J. (2008). Identification practices in government: citizen surveillance and the quest for public service improvement. *Identity in the information society, 1*(1), 135-154

Taylor, P., & Bain, P. (1999). 'An assembly line in the head': work and employee relations in the call centre. *Industrial Relations Journal, 30*(2), 101-117

Tremblay, P., & Lacoste, J. (2003). Crime and innovation: A script analysis of patterns in check forgery. *Crime Prevention Studies, 16*

Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. *Science, 185*(4157), 1124

Commissariat à la protection de la vie privée du Canada, (2010). *Une question de confiance : Intégrer le droit à la vie privée aux mesures de sécurité publique au 21e siècle*. Repéré à www.priv.gc.ca/information/pub/gd_sec_201011_f.cfm#toc6

Vermeij, J. G. (Dir.). (2008). *Security, unpredictability, and evolution*: Berkeley: University of California Press.

Werlinger, R., Hawkey, K., & Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security, 17*(1), 4-19

West, R., Mayhorn, C., Hardee, J., & Mendel, J. (2009). The weakest link: A Psychological perspective on why users make poor security decisions. Dans M. G. e. R. Sharman (dir.), *Social and Human elements of information security: Emerging Trends and countermeasures* (p. 43-60).

Wilkinson, S. (2004). Focus group research. Dans D. Silverman (dir.), *Qualitative research: Theory, method and practice* (2nd Edition[e] éd., p. 177-199). London: Sage.

Workman, M. (2008a). A test of interventions for security threats from social engineering. *Information Management & Computer Security, 16*(5), 463-483

Workman, M. (2008b). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology, 59*(4), 662-674

ANNEXE I

RECHERCHE UNIVERSITAIRE SUR LA FRAUDE D'IDENTITÉ

La **fraude d'identité** est un phénomène émergeant dont les stratagèmes, les motivations ainsi que les conséquences restent pour l'instant incertains.

Depuis quelques années, la direction [redacted] s'intéresse particulièrement aux **tentatives d'accès non autorisées** aux renseignements personnels. Dans l'objectif de mieux comprendre ce phénomène et d'élaborer de mesures de prévention, de détection et d'intervention efficace, la [redacted] s'est associée à l'**École de criminologie** de l'Université de Montréal.

David Castonguay, étudiant à la maîtrise en criminologie, travaille présentement sur l'analyse du phénomène de fraude d'identité et il demande **votre participation** afin de réaliser **un entretien** avec vous.

L'entretien aura lieu **à l'extérieur des heures régulières** de travail, il est d'une durée d'environ 1h30. Il est **anonyme** et **non rémunéré**.

L'**objectif** de cette rencontre est de **dresser un portrait** des stratagèmes utilisés par les fraudeurs potentiels ainsi que d'identifier toutes les **complications** que peut amener l'application du protocole d'identification dans le cadre de votre travail.

À l'aide d'entretiens, nous souhaitons approfondir la compréhension du phénomène criminel afin **d'adapter les mesures de prévention** (formation, sensibilisation) et **de détection** (protocole d'identification, fiche de signalement) déjà en place. Nous désirons également connaître les mécanismes qui sont mis en place par les agents afin de gérer ces situations.

L'objectif de la rencontre est d'utiliser **votre expérience** comme source d'information principale sur le phénomène. Nous souhaitons également connaître **votre opinion** sur les mesures en place et sur les **pistes de solutions** afin d'implanter des mesures de sécurité adaptées à votre travail.

Votre participation est essentielle dans la compréhension du phénomène et dans l'**amélioration** du programme de protection des renseignements personnels déjà en place.

Le lieu de la rencontre sera déterminé lors des communications écrites et verbales avec David.

Vous aimeriez participer? Communiquer avec David par courriel à l'adresse suivante : [redacted] ou par téléphone, au [redacted]

Merci de votre collaboration

École de criminologie
Université de Montréal

ANNEXE II

PLAN D'ENTRETIEN : THÈMES ET QUESTIONS DE RELANCE

Nom :
Prénom :
Date / Heure :
Location :

Description du projet : Bonjour, on s'intéresse aux fraudes d'identité et à la protection des renseignements personnels. Je présente quelques faits sur les tentatives.
Comme vous êtes les mieux placés pour nous parler des complications qui ont lieu lors de l'application du protocole.
On cherche à améliorer ce qui est en place, mais je veux absolument connaître votre point de vue sur la situation. Parce que l'on veut le modifier, c'est vous qui allez l'appliquer. Je vois ça pour vous comme une belle opportunité de me faire part de ce que vous pensez. Ca va me permet de décrire plus mon échantillon de personnes. Tout va rester confidentiel, de toute manière sur le questionnaire, il n'y a pas de nom.

PERCEPTION DES MESURES ET DU PROBLÈME

Protocole d'identification
Parlez-moi de votre appréciation du protocole d'identification.
Comment ça se déroule l'application du protocole?
Qu'est-ce que vous demandez comme identifiants?

Selon-vous est-ce que ça devrait être moins sévère, plus? Est-ce qu'il devrait être modifié? Quels seraient les changements?
Quelles autres questions seraient pertinentes pour identifier la personne? Quelles sont les meilleures qui sont déjà en place?

Type d'appel
Parle-moi un peu des appels que tu reçois habituellement? Type de clientèle est très varié j'imagine? Les demandes doivent être vraiment variée ça peut aller de quoi à quoi?
Quels sont les appels les plus difficiles à gérer pour vous?

Appels suspects
Si on reste un peu dans les complications, avez-vous déjà eu à gérer des appels que vous pensez suspects? Dans le fond, comment savez-vous lorsque quelqu'un essayait de se faire passer pour quelqu'un d'autre? C'est quoi les stratégies qu'il utilise? Quels sont les prétextes leur prétexte?

Décrivez-moi un peu les situations? Par exemple quand la personne raccroche après une question? Est-ce que pour vous c'est une tentative d'accès? Quels autres exemples pouvez nous nous donner.

Quels sont les signes qui vous font douter? Que la vous vous dite c'est bizarre, il y a quelque chose de pas normal? (Temps de réponse, bruit ambiant, voix derrière, tremblement dans la voix, la demande)

Comment faites-vous la distinction entre un échec au protocole et une tentative?

Quelles sont les meilleures questions pour s'assurer que l'on parle à la bonne personne?

Les appels suspects arrivent à quelle fréquence?

Selon vous, quelles sont les motivations de ces personnes?

DILEMME ENTRE PRODUCTIVITÉ ET AUTRES OBJECTIFS

Productivité et sécurité
Combien de temps ça prend environ pour appliquer le protocole?
Est-ce que le protocole entre en conflit avec les objectifs du ministère de traiter les appels plus rapidement? Toi comment tu vois ça, cette opposition? Est-ce que ça change quelque chose à ton travail?
De façon générale comment penses-tu que ce dilemme est vécu par les autres agents?

Formation
Pour répondre à toutes ces demandes, ça demande une bonne formation, combien de temps de formation? Que pensez-vous de l'auto-formation? Comment devrait-elle être utilisée? Quels sont les avantages et désavantages?
Avez-vous des formations pour gérer les appels agressifs? Les cas de suicide? Est-ce que ça vous aide? Ça fait combien de temps que vous l'avez suivi?

Mécanisme refuser l'accès
Au niveau des problèmes rencontrés avec l'application du protocole, ça ressemble à quoi? Comment ça se passe lorsqu'une personne ne réussit pas le protocole? Comment vous lui dite ça? Utilisez-vous une justification? Décrivez un peu le contexte dans ces situations? Réaction du client?

Fiche de signalement
Quelle est votre appréciation de la fiche de signalement? Combien de fois l'avez-vous utilisée? Est-ce qu'il y aurait des pistes d'amélioration?

Autres situations problématiques
Avez-vous d'autres situations complexes dont vous aimeriez me parler?
Comment gérez-vous la situation lorsque quelqu'un ne parle pas la langue?
Est-ce que la règle est efficace? Est-ce que ça permet vraiment

OBSERVATIONS	
Interaction avec le client	
Application des normes	
Environnement de travail	

Rapport d'entrevue (À remplir par David à la suite de chaque entretien)

1. Contexte et déroulement de l'entrevue (présenter le contexte de l'entretien et tout ce qui permet de mieux situer les conditions du discours de l'agent)

2. Remarques méthodologiques (ce qui devrait être mieux défini ou plus approfondi dans une prochaine rencontre, ce devrait être fait et modifié, identifier des sous-thèmes)

3. Compte rendu du contenu de l'entrevue et piste d'analyse (synthèse de ses propos, ce qu'il a dit en gros et des pistes d'analyse et de mise à niveau avec d'autres entrevues).
    a. Attitude générale
    b. Solutions proposées
    c. Problèmes soulevés

4. Analyse transversale (ce qui est semblable et ce qui est différent)
    a. Élément semblable
    b. Élément différent

5. Difficultés générales, impressions, amélioration

ANNEXE III

OBJET : FICHES SIGNALÉTIQUES

Cette annexe présente la compilation des résultats obtenus à l'aide d'un court questionnaire de vingt et une questions distribuées à dix-neuf agents du centre d'appel. Tous les agents avaient préalablement participé à des entretiens avec David Castonguay.

FAITS SAILLANTS

- Les agents rencontrés ont en moyenne **6,1 ans d'expérience**.
- **79%** des agents croient que les politiques de l'organisaion en matière d'accès à l'information ne sont pas claires. (voir question 7)
- **66%** des agents ne trouvent pas la formation en matière *de gestion des appels suspects* est suffisante. (voir question 9)
- **78,9%** des agents trouvent que le **protocole permet de confirmer efficacement** l'identité de la personne (voir question 11)
- **84,2%** des agents ont déjà eu l'impression, même si le protocole d'identification avait été réussi, qu'il avait affaire à un fraudeur (voir question 13)
- **58%** des agents rencontrés **ont déjà utilisé la fiche de signalement** au moins 1 fois. (voir question 15).
- **58%** des agents trouvent que la fiche de signalement est bien adaptée à leur travail (voir question 16)
- Les agents évaluent le nombre d'appels suspect en **moyenne par semaine à 1,52**. (voir question 19)
- **10,5%** des agents rencontrés ont dit que quelqu'un leur avait déjà **offert une rétribution** (argent, cadeau, faveur…) en échange de renseignements personnels qui ne lui appartenaient pas? (par téléphone ou en personne). (voir question 20)
- **5,1%** des agents rencontrés ont dit qu'il avait déjà eu connaissance que l'un de leurs collègues de l'organsation (ancien ou présent) **a déjà accepté une rétribution** (argent, cadeau, faveur…) en échange de renseignements personnels qui ne lui appartenaient pas. (voir question 21)

1. Sexe

☐ Homme **(3)** **(15,8%)**
☐ Femme**(16)** **(84,2%)**

2. Âge

Moyenne de 41,3 ans
Médiane de 42 ans

3. Quel est le dernier niveau de scolarité que vous avez complété?

☐ Secondaire	**(1)**	**(5,3%)**
☐ Diplôme d'études professionnel (DEP)	**(1)**	**(5,3%)**
☐ Attestation d'études collégiales (AEC)	**(0)**	**(0%)**
☐ Technique au niveau collégial	**(3)**	**(15,8%)**
☐ Diplôme d'études collégial général (DEC)	**(6)**	**(31,6%)**
☐ Certificat universitaire	**(2)**	**(10,5%)**
☐ Baccalauréat à l'université	**(5)**	**(26,3%)**
☐ Diplôme de cycle supérieur à l'université	**(1)**	**(5,3%)**
☐ Ne veut pas répondre	**(0)**	**(0%)**

4. En ce moment, poursuivez-vous des **ÉTUDES**?

☐ Non	**(18)**	**(94,7%)**
☐ Oui, j'étudie à temps plein.	**(0)**	**(0%)**
☐ Oui, j'étudie à temps partiel.	**(1)**	**(5,3%)**

5. Votre **EMPLOI** au MESS est :

☐ Temps plein	**(19)**	**(100%)**
☐ Temps partiel	**(0)**	**(0%)**

6. Combien **d'années d'expérience** avez-vous en tant qu'agent aux services à la clientèle dans l'organisation?

Moyenne de : 6,1 ans
Médiane de : 4 ans

7. Est-ce que les politiques de l'organsation en matière d'accès à l'information vous semblent claires et vous aident dans votre travail?

☐ **Tout à fait** d'accord	**(0)**	**(0%)**
☐ **D'accord**	**(4)**	**(21,1%)**
☐ **Pas d'accord**	**(9)**	**(47,4%)**
☐ **Pas du tout** d'accord	**(6)**	**(31,6%)**

8. Quand avez-vous reçu, pour la dernière fois, une sensibilisation/formation concernant *la gestion des appels suspects*?

☐ **Jamais**	**(2)**	**(10,5%)**
☐ Il y a moins de **3 mois**	**(5)**	**(26,3%)**
☐ Il y a moins de **6 mois**	**(7)**	**(36,8%)**
☐ Il y a moins de **9 mois**	**(3)**	**(15,8%)**
☐ Il y a plus de **9 mois**	**(2)**	**(10,5%)**

9. Est-ce que la sensibilisation/formation en matière *de gestion des appels suspects* est suffisante? *

☐ Tout à fait d'accord	**(3)**	**(15,8%)**
☐ D'accord	**(3)**	**(15,8%)**
☐ Pas d'accord	**(9)**	**(47,4%)**
☐ Pas du tout d'accord	**(3)**	**(15,8%)**

*Une personne n'a pas répondu à cette question.

10. Est-ce que la formation que vous avez reçue concernant **l'application du protocole d'identification** est suffisante afin de répondre aux situations que vous rencontrez dans le cadre de votre travail?

☐ Tout à fait d'accord	**(8)**	**(44,1%)**
☐ D'accord	**(6)**	**(31,6%)**
☐ Pas d'accord	**(5)**	**(26,3%)**
☐ Pas du tout d'accord	**(0)**	**(0%)**

11. D'après votre expérience, est-ce que le **protocole d'identification** permet de **confirmer efficacement** l'identité du requérant?

☐ Tout à fait d'accord	**(5)**	**(26,3%)**
☐ D'accord	**(10)**	**(52,6%)**
☐ Pas d'accord	**(4)**	**(21,1%)**
☐ Pas du tout d'accord	**(0)**	**(0%)**

12. Avez-vous déjà oublié d'appliquer partiellement ou totalement le protocole d'identification?

☐ Jamais	**(9)**	**(47,4%)**
☐ Rarement	**(10)**	**(52,6%)**
☐ Parfois	**(0)**	**(0%)**
☐ Souvent	**(0)**	**(0%)**
☐ Toujours	**(0)**	**(0%)**

13. Avez-vous déjà eu l'impression, même si le protocole d'identification avait été réussi, que vous aviez affaire à un fraudeur?

☐ Jamais	**(3)**	**(15,8)**
☐ 1 ou 2 fois	**(14)**	**(73,7%)**
☐ 3 ou 4 fois	**(1)**	**(5,3%)**
☐ 5 fois ou plus	**(1)**	**(5,3%)**

14. Saviez-vous qu'il existe une fiche de signalement concernant les tentatives illégales d'accès renseignements personnels du ministère?

☐ Oui	**(19)**	**(100%)**
☐ Non	**(0)**	**(0%)**

15. Avez-vous déjà **utilisé** cette fiche de signalement?

☐ Jamais	**(8)**	**(42,1%)**
☐ 1 ou 2 fois	**(5)**	**(26,3%)**
☐ 3 ou 4 fois	**(3)**	**(15,8%)**
☐ 5 fois ou plus	**(3)**	**(15,8%)**

16. Cette fiche est-elle **bien adaptée** à votre travail? Je suis :*

☐ Tout à fait satisfait	**(6)**	**(31,6%)**
☐ Satisfait	**(5)**	**(26,3%)**
☐ Peu satisfait	**(3)**	**(15,8%)**
☐ Pas du tout satisfait	**(0)**	**(0%)**

*5 personnes n'ont pas répondu à cette question

17. Avez-vous déjà eu à traiter (répondre) avec un appel suspect? *(Appel suspect : vous avez des doutes raisonnables de croire que l'interlocuteur prétend être quelqu'un d'autre.)*

☐ Oui	**(14)**	**(73,7%)**
☐ Non	**(5)**	**(26,3%)**

18. À combien évalueriez-vous le nombre d'appels suspects que vous recevez **par jour**?

Moyenne de 0,28 appel suspect par jour.
Médiane de 0 appel suspect par jour.

19. À combien évalueriez-vous le nombre d'appels suspects que vous recevez **par semaine**?

Moyenne de 1,52 appel suspect par semaine.
Médiane de 0,5 appel suspect par semaine.

20. Est-ce que **quelqu'un vous a déjà offert une rétribution** (argent, cadeau, faveur…) en échange de renseignements personnels qui ne lui appartenaient pas? (par téléphone ou en personne)*

☐ Oui	**(2)**	**(10,5%)**
☐ Non	**(16)**	**(84,2%)**

*Une personne n'a pas répondu à cette question.

21. Est-ce que vous avez déjà eu connaissance que l'un de vos collègues de l'organsation (ancien ou présent) **a déjà accepté une rétribution** (argent, cadeau, faveur…) en échange de renseignements personnels qui ne lui appartenaient pas.*

☐ Oui **(1)** **(5,3%)**
☐ Non **(17)** **(89,5%)**
*Une personne n'a pas répondu à cette question.